TEKNILLINEN KORKEAKOULU
Sähkötekniikan osasto

Mika Ilvesmäki:

ATM-tekniikan käyttö internet-liikenteen välityksessä

Jätetty tarkastettavaksi: 12.11.1996

Työn valvoja: Professori Raimo Kantola

Työn ohjaaja: TkT Kalevi Kilkki

Tekijä: Mika Ilvesmäki

Työn nimi: ATM-tekniikan käyttö internet-liikenteen välityksessä

Päivämäärä: 12.11.1996 Sivumäärä: 73

Osasto: Sähkö- ja tietoliikennetekniikan osasto

Professuuri: S-38 Teletekniikka

Työn valvoja: Professori Raimo Kantola

Työn ohjaaja: TkT Kalevi Kilkki

Tässä työssä tarkastellaan IP over ATM-, ATM Forum LAN-emulaatio- ja Ipsilon IP-kytkentäratkaisuja internet-verkoissa esiintyvän liikenteen välityksessä. Liikennemittausten avulla tutkitaan näiden teknologioiden soveltuvuutta eri kokoisiin tietoliikenneverkkoihin sekä ATM-välityslaitteistoille asetettavia vaatimuksia. Verkon koko, käyttäjien tottumukset ja käytetyt sovellukset vaikuttavat verkon liikenteen palveluprofiiliin ja asettavat näin ollen aivan erityisiä vaatimuksia ATM-tekniikan tehokkaalle käytölle internet-liikenteen välityksessä. Mittaukset osoittavat, että IP-kytkennän avulla on mahdollista helpottaa reitittimien kuormitusta yli 50 %:lla. Toisaalta liikennevoiden tunnistamiseen, luokitteluun ja kytkentäperusteisiin tulee kiinnittää huomiota, mikäli IP-kytkentää halutaan hyödyntää tulevaisuudessa. Lisäksi IP-kytkinlaitteistojen ja muiden ATM-verkon elementtien väliseen yhteistoimintaan tulee kiinnittää huomiota.

Avainsanat: ATM, B-ISDN, IP-kytkentä, internet, liikennemittaukset, reititys

Author: Mika Ilvesmäki

Name of the thesis: The use of ATM-technology in switching of internet-traffic

Date: 12.11.1996 Number of pages: 73

Faculty: Electrical and Communications Engineering

Professorship: S-38 Telecommunications Technology

Supervisor: Professor Raimo Kantola

Instructor: Dr. Tech. Kalevi Kilkki

Several applications of the ATM-technology in switching and relaying the internet-traffic are studied in this work including IP over ATM, ATM Forum LAN emulation and IP-switching. The applicability of these techniques is resolved through traffic measurements of real computer networks of different magnitude.

Measurements show that traffic and service profiles in the internet are heavily dependent on the size of the network, the habits of the users and the applications used. Measurements indicate that the workload of routers decreases over 50 % if IP-switching is used. On the other hand the identification, classification and the switching criteria of a traffic flow, or an IP-flow, should be further studied to enable the use of IP-switching in different kinds of networks. Also the interoperability between IP-switching equipment and other network components requires special attention.

Keywords: ATM, B-ISDN, IP-switching, internet, traffic measurements, routing

Alkulause

Tämä diplomityö on syntynyt Teknillisen Korkeakoulun Teletekniikan laboratoriossa suorittamani tutkimuksen pohjalta. Tutkimuksessa on perehdytty uusiin ratkaisuihin internet-liikenteen välityksessä sekä selvitetty näiden ratkaisujen ominaisuuksia. Tutkimus on onnekkaasti osunut sellaiseen ajankohtaan, jolloin julkisuuteen on tullut uusia ajatuksia ATM-tekniikan ja internet-liikenteen keskinäisestä vuorovaikutuksesta. On tuntunut erityisen mukavalta tietää olevansa tutkimassa ja selvittämässä uusien asioiden toimivuutta ja soveltamista käytännön elämässä.

Tämän työn valvojaa professori Raimo Kantolaa kiitän tuesta ja kannustuksesta tätä työtä kohtaan. Professori Kantolan oma kiinnostus aihealueeseen loi tämän työn tekemiselle aivan erityisen hyvän pohjan, jolta oli hyvä ponnistaa eteenpäin.

Tämän työn ohjaaja TkT Kalevi Kilkki ansaitsee kiitokset osaavasta ja asiantuntevasta opastuksesta tämän työn aihepiiriin ja erityisesti perehdyttämisestä liikennemittausten maailmaan ja näistä saatujen tulosten esiinkaivamiseen.

Lisäksi tahdon kiittää Teletekniikan laboratorion esimiestä professori Timo Laaksoa innostavan ja myönteisen ilmapiirin luomisesta laboratorioon, sekä kaikkia laboratorion henkilökuntaan kuuluvia toimivan ja asiallisen tutkimusympäristön luomisesta.

Aivan viimeiseksi osoitan kiitokseni Kirsille, joka on kärsivällisesti jaksanut kuunnella ääneenajatteluani. Ilman hänen aurinkoista hymyään ja kannustustaan tämä työ ei olisi koskaan valmistunut.

Espoossa 12.11.1996

Mika Ilvesmäki

Sisällysluettelo

Kuvaluettelo

Taulukkoluettelo

Symboli- ja lyhenneluettelo

AAL	ATM Adaptation Layer, ATM sovituskerros.
ABR	Available Bit Rate, palveluluokka, jossa 'päästä-päähän' -vuonohjaus.
ATM	Asynchronous Transfer Mode, asynkroninen toimintamuoto.
ATM NIC	ATM Network Interface Card. Verkkokortti, joka tarjoaa rajapinnan ATM-tekniikkaa käyttävään tietokoneverkkoon.
ATMARP	ATM Address Resolution Protocol, ATM-osoitteen selvitysprotokolla.
B-ISDN	Broadband Integrated Services Network, laajakaistainen digitaalinen monipalveluverkko.
BUS	Broadcast and Unknown server. ATM Forum LAN-emulaation monilähetyspalvelin.
CAC	Connection Admission Control, yhteyden hyväksymismenettely.
CBR	Constant Bit Rate, palveluluokka, joka takaa tasaisen siirtonopeuden ATM-verkossa.
CDV	Cell Delay Variation, solun siirtoviiveen vaihtelu.
CLP	Cell Loss Priority, soluhukan todennäköisyys.
CLR	Cell Loss Ratio, soluhukkasuhde.
CP PDU	Common Part Protocol Data Unit, AAL-sovituskerroksen yhteisosan tietoyksikkö.
CPI	Common Part Indicator, AAL-5 sovituskehyksen osa.
CRC	Cyclic Redundancy Check, tarkistussumma.
CTD	Cell Transfer Delay, maksimi solun siirtoviive.
GFC	Generic Flow Control, vuon ohjaus.
GSMP	General Switch Management Protocol, yleinen ATM-kytkentälaitteen hallintaprotokolla.
HEC	Header Error Correction, otsikon virheen korjaus.
HTTP	Hypertext Transfer Protocol, Hypertekstin siirtoprotokolla.
IFMP	Ipsilon Flow Management Protocol, Vuon hallintaprotokolla.
InATMARP	Inverse ATM Address Resolution Protocol, käänteinen

	ATMARP-protokolla.
IP over ATM	Protokollapino, jonka avulla IP-liikennettä voidaan välittää ATM-verkoissa; käytetään myös nimeä classical IP over ATM.
IP, IPv4	Internet protocol, internet-liikenteen verkkoprotokolla.
IPv6, IPng	Internet Protocol v6, next generation, internet-liikenteen uudistettu verkkoprotokolla.
ISDN	Integrated Services Digital Network, digitaalinen monipalveluverkko.
ITU-T	International Telecommunications Union - Telecommunications Branch. Kansainvälinen telealan standardointielin.
LAN	Local Area Network, lähiverkko.
LAN-emulaatio	ATM Forumin kehittämä menetelmä yhteydettömien lähiverkkopalvelujen tarjoamiseksi ATM-verkossa.
LEC	Lan Emulation Client, ATM Forum LAN-emulaatioverkon asiakas.
LECS	Lan Emulation Configuration Server, ATM Forum LAN-emulaatioverkon määrittelypalvelin.
LES	Lan Emulation Server, ATM Forum LAN-emulaatioverkon palvelin.
LLC	Logical Link Control, siirtoyhteyskerroksen hallintamenettely.
MAC	Medium Access Control, fyysisen tason hallintamenettely.
MAN	Metropolitan Area Network, kaupunkiverkko.
Multicast	Monilähetys.
NNI	Network-Network Interface, Node-Node Interface, verkon kytkentäelementtien välinen rajapinta.
NPC	Network Parameter Control, verkkoparametrien valvonta.
PAD	Padding, täytebitti.
PTI	Payload Type Identifier, hyötykuorman tyypin tunniste.
PVC	Permanent Virtual Connection, kiinteä virtuaaliyhteys.
QoS	Quality of Service, yhteyden laatutaso.
RSVP	Resource Reservation Protocol, verkon resurssien varausprotokolla.

SNAP	SubNet Access Point. Aliverkon liittymispiste.
SVC	Switched Virtual Connection, kytkentäinen virtuaaliyhteys.
TCP	Transmission control protocol, internet-verkkojen yhteydellinen pakettivälitysprotokolla.
UBR	Unspesified Bit Rate, palveluluokka, jolle ei ole määritetty yhteysnopeutta.
UDP	User Datagram Protocol, internet-verkkojen yhteydetön pakettivälitysprotokolla.
UNI	User Network Interface, käyttäjän ja verkon välinen rajapinta.
UPC	User Parameter Control, käyttäjäparametrien valvonta.
UU	User to User, käyttäjältä-käyttäjälle.
WAN	Wide Area Network, laajoja alueita yhdistävä tietokoneverkko.
VBR	Variable Bit Rate, palveluluokka, joka tarjoaa vaihtelevannopeuksista yhteyttä.
VCI	Virtual Channel Identifier, virtuaalikanavan tunniste.
VoD	Video on Demand, tilausvideopalvelu.
VPI	Virtual Path Identifier, virtuaaliväylän tunniste.

Johdanto

ATM-tekniikan käyttöönotossa tärkeä vaihe on käytössä olevien tietokoneverkkojen vaivaton muuttaminen ATM-tekniikkaa - osittain tai kokonaan - hyödyntäviksi verkoiksi. Ei kuitenkaan ole taloudellisesti realistista olettaa, että laitteistot ja ohjelmistot uusittaisiin yhtäaikaisesti uuden teknologian tullessa markkinoille. Internet-verkkojen palvelujen monipuolistuessa, käytön kasvaessa ja käyttäjien määrän lisääntyessä erilaiset suurta siirtokaistaa vaativat palvelut nostavat internet-protokollien välityskysymykset merkittäväksi ongelmaksi myös ATM-verkoissa. Internetissä käytettäviä protokollia täytyy kyetä välittämään sujuvasti myös ATM-verkoissa.

Tämän työn tavoitteena on esitellä ATM-tekniikan erilaisia soveltamistapoja internet-protokollien välityksessä ja tutkia näiden tekniikoiden soveltuvuutta eri kokoluokkaa oleviin tietoliikenneverkkoihin. Lisäksi tämän työn tarkoituksena on kartoittaa erikokoisissa internet-protokollia käyttävissä tietoliikenneverkoissa esiintyviä liikennevirtoja sekä tutkia ja selvittää edellytyksiä ja reunaehtoja erilaisten ATM-tekniikan soveltamistapojen käyttöön näissä verkoissa. Edelleen perehdytään mahdollisuuteen käyttää kytkentäisiä yhteyksiä internet-liikenteen välityksessä verkon palvelutason nostamiseksi.

Työssä luodaan yleiskatsaus erityyppisiin käytössä oleviin ATM-tekniikkaa internet-verkoissa käyttäviin menetelmiin sekä selvitetään näiden etuja ja heikkouksia. Lisäksi esitetään todellisissa tietoliikenneverkoissa tehtyjä liikennemittauksia ja pohditaan esitettyjen välitystekniikoiden mahdollista vaikutusta liikenteeseen ja verkon kuormitukseen sekä niitä vaatimuksia, joita näiden välitystekniikoiden käyttö asettaa välityslaitteistolle.

Ensimmäisessä luvussa käydään läpi ATM-tekniikan perusteita, perehdytään yleisesti yhteyden käsitteeseen ATM-verkoissa sekä yhteyksien muodostamiseen ja käsittelyyn ATM-verkoissa.

Toisessa luvussa tarkastellaan keskeisimpien internet-protokollien rakennetta ja pohditaan näiden ominaisuuksia välitystekniseltä kannalta.

Kolmannessa luvussa perehdytään IP over ATM-malliin. Tämä malli on usean nykyisen ATM-tekniikkaa käyttävän internet-liikenteen välitysjärjestelmän pohjaratkaisuna.

Neljännessä luvussa perehdytään ATM Forumin kehittämän lähiverkkoemulaation tarjoamiin mahdollisuuksiin internet-protokollien välityksessä. Lähiverkkoemulaatio on saavuttanut vahvan aseman siirryttäessä perinteisistä lähiverkkoteknologioista ATM-tekniikan hyväksikäyttöön lähiverkoissa.

Viidennessä luvussa perehdytään mahdollisuuksiin yhdistää perinteinen internet-reititin ja ATM-tekniikka. Tässä yhteydessä tutustutaan yhteen kaupalliseen ratkaisuun tästä ajatusmallista.

Kuudennessa luvussa tutkitaan mittausten avulla erään pienen, keskikokoisen ja suuren internet-protokollia kuljettavan verkon liikenteen koostumusta ja pohditaan kytkentäisen ATM-tekniikan käytön vaikutuksia kytkentälaitteiston ja verkkoresurssien käyttöön.

1 ATM

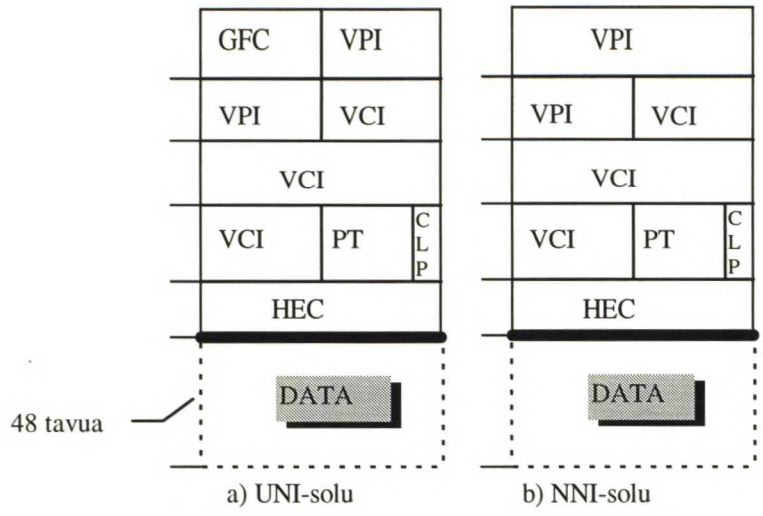
1.1 Yleistä

ITU-T (International Telecommunications Union - Telecommunications branch) aloitti vuonna 1988 laajakaistaisen monipalveluverkon (Broadband Integrated Services Digital Network, B-ISDN) siirtomuodon standardisoinnin. Siirtomuodoksi valittiin uudenlainen tapa toteuttaa kytkentäinen pakettivälitysjärjestelmä. Nämä standardit määrittelivät B-ISDN-verkkojen kytkentä- ja välitystekniikan ja tämä uusi tekniikka nimettiin asynkroniseksi siirtomuodoksi (Asynchronous Transfer Mode, ATM). Tarkoituksena on pystyä välittämään B-ISDN-verkoissa ATM-tekniikan avulla samanaikaisesti siirtokapasiteetin käytön suhteen hyvin erilaisia telepalveluja hyödyntäen kuitenkin verkkoresursseja mahdollisimman optimaalisesti. ATM-tekniikassa tieto välitetään pieninä vakiomittaisina paketteina, soluina, jotka siirretään aikajakoisen välitysjärjestelmän eri aikaväleissä asynkronisesti eli yksittäisen tietovuon soluille ei ole määritelty vain yhtä aikaväliä, vaan ne voivat käyttää yhteydelle määritetyn liikennöintisopimuksen puitteissa siirtokapasiteettia vapaasti. Aikavälit tunnistetaan ATM-solun otsikkotiedon perusteella. Asynkronisuudella tarkoitetaan ATM-tekniikan yhteydessä siis dynaamista kaistanleveyden jakoa yhteyksien ja käyttäjien välillä. /1/

ATM-tekniikan kehitystyö jatkuu edelleen ja tähän työhön osallistuu useita eri yhteisöjä. Näistä tärkeimpinä voidaan mainita ITU-T ja pääosin eurooppalaisten ja pohjois-amerikkalaisten yritysten muodostama epäkaupallinen yhteenliittymä ATM Forum.

1.2 ATM-solu

ATM-tekniikassa pienin siirrettävä tietoyksikkö on solu. ATM-solut muodostuvat 5 otsikkotavusta ja 48 tavusta siirrettävää tietoa. Päätelaitteen ja verkon rajapinnalla (User to Network Interface, UNI) sekä verkkojen välisillä rajapinnoilla (Network to Network Interface, NNI) käytettävien solujen sisäinen rakenne eroaa hieman toisistaan. Kuvassa 1-1 on esitetty solurakenne eri rajapinnoilla. Kuvassa yksi rivi vastaa yhtä tavua eli 8 bittiä.



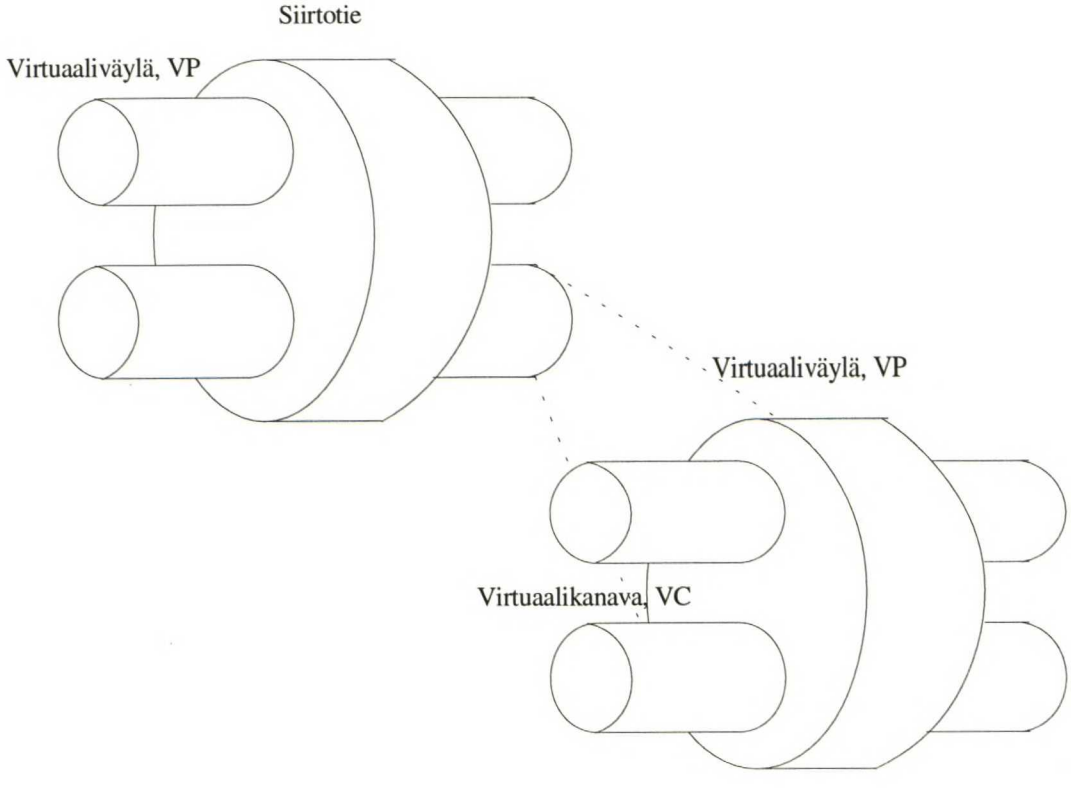
Kuva 1-1: ATM-solun rakenne /2/

Ainoa ero NNI-solun ja UNI-solun rakenteessa on vuonohjauskentän (Generic Flow Control, GFC) puuttuminen edellisestä. Otsikon tiedoista suurimman osan (3 tavua UNI-solussa ja 3,5 tavua NNI-solussa) vievät virtuaaliväylien ja -kanavien tunnistekentät (Virtual Path Identifier, VPI ja Virtual Channel Identifier, VCI), jotka määrittelevät solu siirtotien ATM-verkossa. Näiden kenttien arvot eivät ole absoluuttisia yhdellä yhteydellä, sillä ATM-välityslaitteistot muuttavat VPI- ja VCI-kenttien arvoja omien reititystaulukkojensa mukaan. Hyötykuorman tunnistekentän (Payload Type, PT) avulla erotetaan verkon hallintatietoja tai muuta erityisinformaatiota sisältävät solut. Erityisesti PT-kentän avulla voidaan tiedottaa ATM-välityslaitteistossa tai -verkossa havaitusta tai uhkaavasta estosta. Solun hukkaamiskenttä (Cell Loss Priority, CLP) määrittää onko solu ensisijaisesti pyrittävä säilyttämään vai voidaanko sen välittämisestä estotilanteessa tai eston uhatessa luopua. Otsikon tarkistussumman (Header Error Control, HEC) avulla pyritään havaitsemaan virheet solun otsikkotiedoissa. Yhden solun otsikkokentän jälkeen seuraa aina 48 tavua käyttäjän tietoa (kuvassa 1-1 DATA-kenttä), jonka sisällön oikeellisuuteen tai virheettömyyteen ATM-välityslaitteisto ei ota kantaa. /1, 2, 3, 4/

1.3 Yhteydet ATM-verkoissa

ATM-verkot ymmärretään tässä työssä sellaisiksi tietoliikenneympäristöiksi, joissa verkkoliikennettä välitetään ATM-tekniikan avulla. Erityisesti on huomattava, että suurissa runkoverkoissa ei välttämättä käytetä yksinomaan ATM-tekniikkaa,

vaan tiedonvälitys toteutetaan yhdessä ATM-tekniikan ja synkronisten siirtotekniikoiden (SONET, SDH) avulla, jolloin ATM-soluja kuljetetaan synkronisten siirtotekniikoiden kuljetuskehyksissä /1/. ATM on yhteydellinen eli kytkentäinen tekniikka ja solut säilyttävät lähetysjärjestyksensä toisiinsa nähden yhteyden päästä päähän. ATM-välityslaitteisto muodostaa yhdessä päätelaitteiden ja toisten ATM-välityslaitteistojen kanssa yhteyksiä. Käytännössä yhteyksiä muodostetaan merkinantoprotokollien tai muiden verkonhallintamenetelmien avulla. Yhteydet jaetaan virtuaaliväyliin (virtual path, VP) ja virtuaalikanaviin (virtual channel, VC). Virtuaaliväylät jakavat siirtotien tarjoaman siirtokaistan ja sisältävät useampia virtuaalikanavia. Virtuaaliväylien pääasiallinen merkitys on ohjata suuria liikennevirtoja ja helpottaa reitityksen toteuttamista ATM-verkoissa (kuva 1-2). Virtuaalikanavat muodostavat varsinaisen yhteyden toistensa kanssa kommunikoivien sovellusten välille. /1, 2/



Kuva 1-2: Virtuaaliväylät ja kanavat/looginen tarkastelu

Väylät ja kanavat voidaan muodostaa joko manuaalisesti verkonhallinnan avulla, jolloin kyseessä ovat pysyvät virtuaaliyhteydet (Permanent Virtual Connection, PVC) tai merkinannon avulla, jolloin kyseessä ovat kytkentäiset virtuaaliyhteydet

(Switched Virtual Connection, SVC). Kytkentäisten virtuaaliyhteyksien purkaminen tapahtuu niinikään merkinannon avulla yhteyden päättyessä.

Sekä pysyviin että kytkettyihin yhteyksiin liittyy ATM-tekniikassa käsite palvelun laatu (Quality of Service, QoS). Jokaiselle yhteydelle voidaan määrittää oma QoS, kuitenkin siten että yksittäisen virtuaaliväylän sisällä kulkevilla virtuaaliyhteyksillä on sama tai huonompi palvelun laatu kuin väylällä. Palvelun laatu määritetään ennen varsinaista yhteydenmuodostusta CAC-mekanismin (Connection Admission Control, CAC) avulla. CAC-mekanismi neuvottelee yhteyden aloittavan osapuolen kanssa yhteysparametreistä (taulukko 1-1) ja päättää viime kädessä, voidaanko yhteys muodostaa aiheuttamatta mahdollisesti yhteyden laadun huononemista muilla, jo olemassaolevilla, yhteyksillä. Yhteyden palvelutasoa ei yleensä ole mahdollista muuttaa kesken yhteyden. Standardointityö tällaisten ominaisuuksien lisäämiseksi on tosin käynnissä. Lisäksi on huomattava, että kaikkiin edempänä esitettäviin palveluluokkiin (taulukko 1-2, UBR ja ABR) ei ole mahdollista sopia palvelun laadun tasoa sovellusten muodostaessa yhteyttä ja CAC-mekanismin tehtäväksi jää tehdä päätös siitä, voidaanko yhteyttä ylipäätään muodostaa.

Taulukko 1-1: QoS-parametrit

Parametri	Lyhenne
Huipusta huippuun soluviiveen vaihtelu	peak-to-peak CDV
Solun maksimi siirtoviive	maxCTD
Soluhukkasuhde	CLR

Verkon suurista nopeuksista, pienestä solukoosta ja pyrkimyksistä pieniin puskurikokoihin ATM-välityslaitteistoissa johtuu, että perinteistä takaisinohjautuvaa vuonohjausta ei pidetä hyvänä ensisijaisena menetelmänä liikennevirtojen valvonnassa. ATM Forum on kuitenkin kehittänyt ABR-palvelun (available bit rate), jossa vuonohjaus toimii yhteyden eri osapuolien välillä. Kaikissa liikenneluokissa, joille on määritelty palvelun laatu, UPC/NPC (User tai Network Parameter Control) -komponentti valvoo liikennöintisopimusten pysymistä sovituissa rajoissa liikennöinnin aikana. /1/

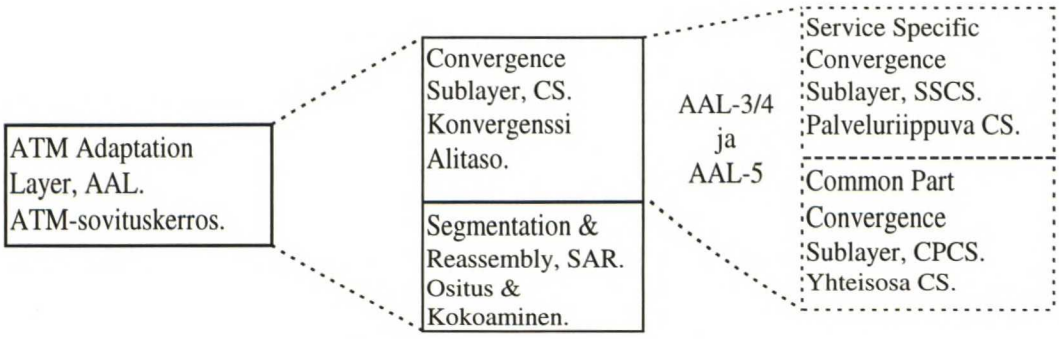
1.4 Tiedon siirtomuodot

ATM-verkon tarjoamaa siirtopalvelua ei käytetä suoraan. Siirrettävää tietoa käsitellään erilaisten ATM-sovituskerrosten avulla (ATM Adaptation Layer, AAL). ATM Forumin /5/ mukaan palveluluokat ja niihin soveltuvat käyttäjän sovellukset sekä ATM-sovituskerrokset jakautuvat tällä hetkellä taulukon 1-2 mukaan.

Taulukko 1-2: ATM-tason palveluluokat ATM- Forumin mukaan /5/:

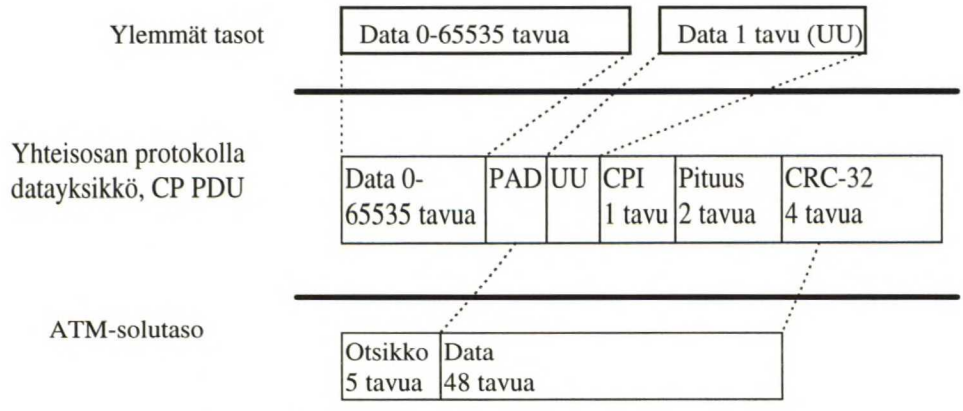
Palveluluokka	**Käyttösovellus/Käyttövaatimus**	**ATM sovituskerros, AAL**
CBR, Constant Bit Rate	Videokonferenssi, VoD, Puhelin; tasaista nopeutta vaativat	AAL-1
rt-VBR, real time Variable Bit Rate	Kompressoitu kuva ja ääni; muut tilastollista kanavointia hyödyntämään kykenevät sovellukset	AAL-3/4
nrt-VBR, non-real time Variable Bit Rate	Prosessinvalvonta, pankki- yms. Sovellukset	AAL-3/4
UBR, Unspecified Bit Rate	Sähköposti, tiedostonsiirto, LAN-emulaatio	AAL-5
ABR, Available Bit Rate	Tietoliikennesovellukset; ABR-vuonohjausta hyödyntämään kykenevät sovellukset	AAL-5

Siirrettäessä ATM-verkossa suurempia tietoyksikköjä kuin 48 tavua täytyy tieto sovittaa ATM-sovituskerroksen toimintojen avulla siirtotielle. AAL-sovituskerros voidaan jakaa kahteen osaan, joista ylempi taso voidaan tarvittaessa jakaa edelleen kahteen osaan (kuva 1-3). Tämä jako on toteutettu AAL-3/4 ja AAL-5 sovituskerrosten kohdalla.



Kuva 1-3: AAL-sovituskerroksen rakenne /1/

AAL-sovituskerroksen SAR-alitaso (Segmentation And Reassembly) jakaa tiedon soluihin ja toisaalta kokoaa saapuneet solut kokonaisiksi informaatioyksiköiksi. CS-alitaso (Convergence Sublayer) huolehtii välitettävän tiedon muusta sovittamisesta. Käytettäessä AAL-3/4 tai AAL-5 sovituskerrosta CS-alitaso on edelleen jaettu palveluspesifiseen ja yhteiseen osaan. Internet-liikenteen välityksessä ainoastaan AAL-5 sovituskerros on merkittävässä asemassa. AAL-5 sovituskerros on rakenteeltaan yksinkertainen ja se tukee vaihtelevanopeuksista liikennettä ATM-verkoissa. AAL-5 sovituskerroksen yhteisosa takaa virheet havaitsevan yhteydellisen siirtotien vaihtelevanmittaisille tietokehyksille. AAL-5 ei tue useamman ylemmän tason sovelluksen yhteyksien sovittamista kuten esimerkiksi AAL-3/4. AAL-5 yhteisosan (AAL-5 CP) muodostuminen on esitetty kuvassa 1-4.



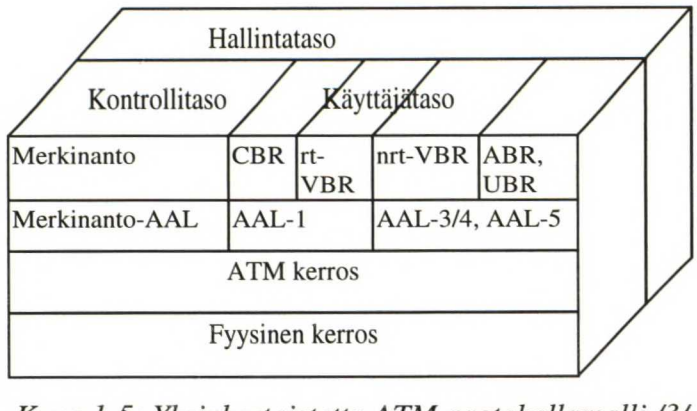
Kuva 1-4: AAL-5 CP:n muodostuminen /1/.

AAL-5 yhteisosan protokollatietoyksikkö (Common Part Protocol Data Unit, CP PDU) rakentuu käyttäjän lähettämän varsinaisen tiedon lisäksi täytetavuista (0-47 kpl, PAD), jotka tekevät yhteisosan protokollayksiköstä täsmälleen 48 tavun monikerran. AAL-5 kehyksessä on myös mahdollisuus siirtää käyttäjältä toiselle lisä-

informaatiota yhden tavun (UU-kenttä) verran yhdessä AAL-5 kehyksessä. Tällä hetkellä tälle toiminteelle ei ole käyttöä, mutta tulevaisuudessa sitä tullaan mahdollisesti käyttämään lyhyiden merkinantotyyppisten sanomien välittämiseen käyttäjältä toiselle. Yhteisosan indikaattorille (CPI, Common Part Indicator, 2 tavua) ei myöskään tällä hetkellä ole standardoitua käyttöä ja se on varattu tulevaa käyttöä varten. Yhteisosan protokollatietoyksikön lopussa on varattu kaksi tavua PDU:n koon ilmoittamiseksi ja neljä tavua CRC-32 menetelmällä laskettua tarkistussummaa varten. Tarkistussumma lasketaan koko CP PDU-kehyksestä. Yhteisosan protokollakentän viimeinen solu havaitaan tarkkailemalla ATM-solujen PT-kenttää. PT-kenttä saa yhteisosan protokollakentän viimeisessä solussa, mikäli verkossa ei ole estoa, binäärisen arvon 001 tai, mikäli verkossa on havaittu estoa, binäärisen arvon 011. /1/

1.5 Yhteenveto

ATM-tekniikka on monipuolinen yhteydellinen tiedonsiirtomenetelmä, jossa kaikki ATM-verkon tietovirrat - käyttäjä-, kontrolli- ja hallintatiedot - kulkevat samassa välitysjärjestelmässä (kuva 1-5). ATM-tekniikan avulla pystytään tarjoamaan käyttäjän tarpeen mukaisesti joustava kaistanleveys erilaisten palveluluokkien avulla hyvin erilaisille palveluille. On kuitenkin huomattava, että monilähetysliikenteen välitys, jossa yksi lähettäjä lähettää monelle vastaanottajalle tai useat käyttäjät lähettävät useille käyttäjille, on muodostunut ongelmaksi käytettäessä ATM-tekniikkaa. Perusajatukseltaan yhteydellisessä ympäristössä tämä muodostaa haasteellisen ongelman, jonka ratkaisemiseksi kehitetty erilaisia ratkaisuja, joista muutamia sivutaan seuraavien lukujen yhteydessä.



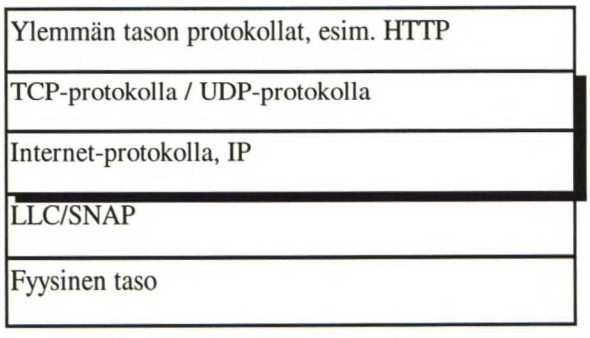
Kuva 1-5: Yksinkertaistettu ATM-protokollamalli /3/

Lisäksi ATM-tekniikan ongelmiksi ovat muodostuneet käytännön toteutusten monimutkaisuus ja sovelluksissa tarvittavien protokollakerrosten runsaus. Tämä johtuu osittain siitä, että ATM-teknologiaan siirtyminen ei saa tuottaa käyttäjälle liikaa näkyviä muutoksia. Tällä hetkellä ongelman muodostaa resurssien jaon ja käytön valvonnan toteutus. Perinteisissä kytkentäisissä yhteyksissä aikavälin ollessa varattu yhdelle yhteydelle on valvonta yksiselitteistä, mutta ATM-tekniikassa yhtä aikaväliä voivat vuoronperään käyttää eri yhteydet ja verkon valvonnan toteuttaminen saattaa muodostua hyvin vaikeaksi tehtäväksi. Niinikään eri palveluluokkien välisten suhteiden määrittely esim. laskutuksessa on tällä hetkellä tutkimuksen kohteena. Kaikille edellämainituille ongelmille tulee löytyä ratkaisu ennen kuin ATM-tekniikkaa voidaan soveltaa laajamittaisesti yleisissä verkoissa.

2 Internet-protokollat

2.1 Yleistä

Internetillä ymmärretään tässä työssä sellaisia tietoliikenneratkaisuja, joiden avulla erillisten tietokoneverkkojen, yleensä lähiverkkojen, yksittäiset jäsenet pystyvät tarvittaessa kommunikoimaan keskenään - tästä on johdettu internetin arkinimitys: 'verkkojen verkko'. Internet syntyi USA:ssa 1970-luvun alussa. Protokollien kehitystyön aloitti USA:n puolustusministeriö (Department of Defense, DoD). Tarkoituksena oli rakentaa sodan koettelemuksia kestävä tietoliikenneverkko, jossa tiedon varma perillepääsy monitoimittajaympäristössä oli ensisijaista. Tiedonsiirrossa käytettävien protokollien täytyi näinollen pystyä välittämään tieto perille erittäin varmasti ja virheettömästi laitteistoympäristöistä ja verkon fyysisen rakenteen dynaamisuudesta huolimatta. Lisäksi protokollien käytön edellytyksenä ei haluttu vaatia keskitettyä verkonhallintamekanismia. Syntynyt protokollaperhe tunnetaan nykyään internet-protokollaperheenä (IP-protokollat) ja protokollat ovat levinneet maailmanlaajuiseen käyttöön internetin laajenemisen yhteydessä. Kuvassa 2-1 on esitetty internet-protokollien sijoittuminen suhteessa muihin tiedonsiirrossa yleisesti käytettyihin protokolliin ja menettelyihin.

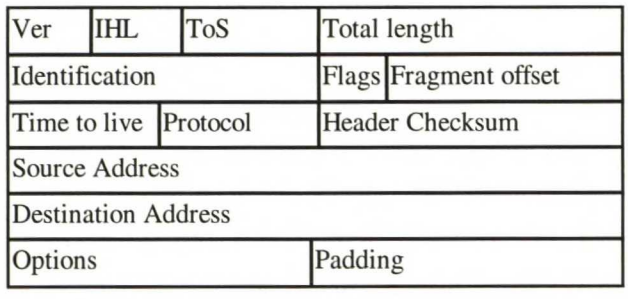


Kuva 2-1: Internet-protokollien sijoittuminen /4/

Protokollaperhe on saavuttanut de-facto standardiaseman erilaisten internet-verkkojen välitysprotokollana. Perusajatuksena protokollaperheessä on yhteydetön tiedonsiirto eri osapuolten välillä ja verkkojen välinen kommunikaatio (internet working) reitittimien ja siltojen avulla. Yhteydellisyys on IP-protokollapinossa siirretty mahdollisimman korkealle tasolle ja IP-protokollat eivät edellytä siirtotieltä aivan yhtä suurta varmuutta ja virheettömyyttä kuin ATM-tekniikka. /4/

2.2 Internet protokolla - IP

IP-protokolla (Internet Protocol; myös IPv4) on yhteydetön siirtoprotokolla pakettikytkentäisissä verkoissa. IP-protokolla tarjoaa tietopakettien lähetys- ja vastaanottopalvelun ja tarvittaessa tietopakettien pilkkomisen ja kokoamisen kahden osapuolen välillä. IP-protokolla pystyy tarvittaessa tukemaan erilaisia palveluluokkia ja -tasoja, mutta tällaisia ratkaisuja ei olemassaolevissa verkkoratkaisuissa ole toteutettu. IP-protokolla ei takaa tiedon luotettavaa siirtoa yhteydellä, joten siirrettävän tiedon oikeellisuus tulee aina tarkistaa ylemmän tason yhteydellisen protokollan avulla. IP-kehyksen rakenne on esitetty kuvassa 2-2. Kuvassa yksi rivi muodostuu neljästä tavusta eli 32 bitistä.



Kuva 2-2: IP-kehyksen rakenne /6/

ToS-kenttä määrittää palvelutyypin (Type of Service) ja tietopaketin kohtelun verkossa prioriteetin, viiveen, läpäisyn (throughput) ja luotettavuuden avulla. Palvelutyypit on esitetty taulukossa 2-1.

Taulukko 2-1: IP-protokollan palvelutyypit /6/

Parametri (ja pituus bitteinä)	**Vaihtoehdot**
Prioriteetti (3 bit)	Yhdeksän eri vaihtoehtoa
Viive (1 bitti)	Normaali (0) ja Matala (1)
Läpäisy (1 bitti)	Normaali (0) ja Korkea (1)
Luotettavuus (1 bitti)	Normaali (0) ja Korkea (1)

Vaikka IP-kehyksessä onkin siis määritelty kohtuullisen monitasoinen palvelun laadun määrittelyn mahdollistava ominaisuus, sitä ei ole juurikaan toteutettu verkkoympäristöissä. Perussyynä tähän on se, että edelleen yleisesti käytössä olevat paikallisverkkoteknologiat (Ethernet, Token Ring) eivät pysty takaamaan tiettyä

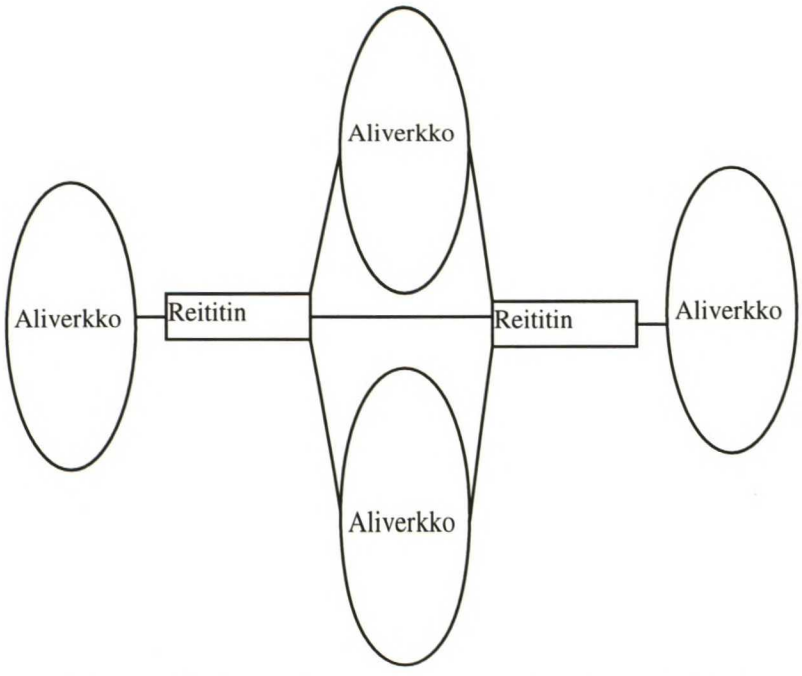
palvelutasoa ja mikäli yhteydellä on yksikin verkkosegmentti, joka ei pysty palvelun tasoa takaamaan, ei palvelun tasoa yhteydellä voida tarkasti määritellä tai taata.

Time to live-kenttä määrittää kuinka kauan pakettia käsitellään verkossa. Elinaika on standardissa määritelty sekunneissa, mutta joka kerta kun pakettia käsitellään verkossa kentän arvosta vähennetään yksi, joten käytännössä kyseessä on paketin elinajan määritys käsittelykertojen lukumääränä. Mikäli kentän arvo on nolla, paketti tuhotaan, eikä sitä välitetä eteenpäin. Protocol-kenttä ilmaisee mitä protokollaa ylemmällä tasolla välitetään. Otsikon tarkistussummakenttä (Header Checksum) pyrkii takaamaan otsikkotietojen oikeellisuuden. Options-kentässä voidaan lähettää erilaisia reititykseen liittyviä komentoja sekä mahdollisesti ajastukseen liittyvää tietoa (timestamp).

Liikenteen välityksen kannalta oleellisinta IP-kehyksen otsikossa on lähettäjän ja vastaanottajan IP-osoitekentät (Source ja Destination Address). Näiden kenttien avulla verkon eri komponentit, lähinnä reitittimet, päättelevät miten IP-kehys toimitetaan haluttuun määränpäähänsä. Tämä toiminta muodostaa internet-verkkojen erään oleellisimman toiminnon, reitityksen. /6/

2.2.1 Reititys

Internet-verkot koostuvat useista aliverkoista. Näiden aliverkkojen loogisille reunoille on sijoitettu reitittimet, joilla on vastuu IP-kehysten ohjaamisesta, reitityksestä, verkkojen välillä. Tätä rakennetta selvittää kuva 2-3.



Kuva 2-3: Internetin rakenne ja reitittimien sijainti

Reitittimet päättelevät IP-kehyksen osoite-kenttien ja reititystaulukoidensa avulla mihin IP-kehys tulee lähettää. Reititys perustuu usein ns. etäisyysvektorien laskemiseen. Tällöin määritellään tietyn parametrin suhteen edullisin reitti kohteeseen. Reitin edullisuuden kriteeriksi voidaan valita useita suureita: Yleisesti käytössä olevia edullisuustekijöitä ovat muunmuassa kulkuaika ja kustannukset. Reitin löytämiseksi on käytössä useita erilaisia menetelmiä, joista muutamia on lyhyesti esitelty taulukossa 2-2.

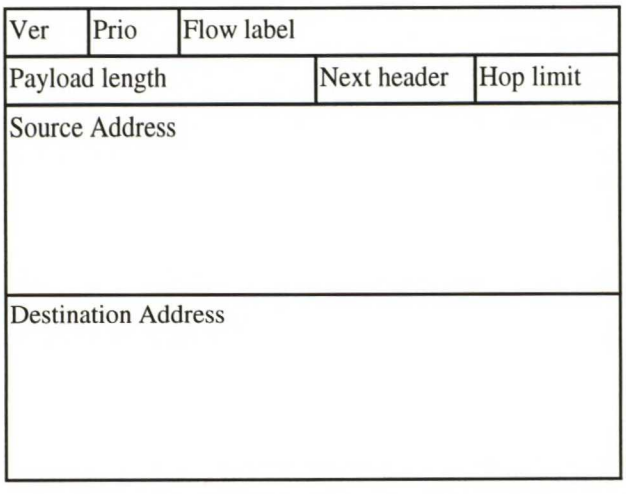
Taulukko 2-2: Internet-reititysprotokollia /7/

Reititysprotokollan nimi	**Käyttötarkoitus**
Routing Information Protocol, RIP	Perusmenetelmä reitin löytämisessä, hyödyntää etäisyysvektorimenetelmää (Distance Vector Algorithm).
Classless InterDomain Routing, CIDR	Uusi menetelmä reitin etsimiseen, ei ole riippuvainen IP-osoitteiden luokista. Soveltuu ns. autonomisten systeemien välillä tapahtuvaan reititykseen.
Open Shortest Path First, OSPF	Tehokas reititysprotokolla, joka perustuu Dijkstran algoritmien hyödyntämiseen. Selvittää ympäröivän verkon rakenteen ns. tulva-menetelmällä. Soveltuu ns. autonomisten systeemien sisäiseen reitittämiseen.
Border Gateway Protocol, BGP	Reititysprotokolla ns. autonomisten systeemien välillä tapahtuvaan reitittämiseen.
Distance Vector Multicast Routing Protocol, DVMRP	Käytetään multicast-viestien reititykseen. Soveltuu vain ns. autonomisten systeemien sisäiseen reitittämiseen.

Reititysprotokollien avulla varmistetaan tiedon luotettava siirtyminen yhteydellä. Protokollien tarkoitus on on selvittää millainen on ympäröivän verkon looginen rakenne ja näin taata esimerkiksi vikatilanteissa vaihtoehtoisen reitin löytyminen. Reitittimien tiedonkäsittelykapasiteetilta vaaditaan paljon. Siirtotekniikan kehittyessä ja uusien teknologioiden tultua markkinoille reitittimien kapasiteetti muodostaa tällä hetkellä pahimman pullonkaulan internet-liikenteen välityksessä. /7,8/

2.2.2 IPv6 - uusi internet protokolla

IP-protokollan ominaisuudet on internetin voimakkaan kasvun takia havaittu joiltakin osin puuteellisiksi ja tämän takia IP-protokollasta on kehitetty uusi versio, joka tunnetaan nimellä IPv6 tai IPng. IPv6-protokollan parannettuina ominaisuuksina vanhaan IP-protokollaan verrattuna ovat laajennettu IP-osoiteavaruus, tehostetut reititystoiminnot, mahdollisuus identifioida tietovoita ja määrittää palvelun laatu yhteydellä sekä parannetut mahdollisuudet tietoturvan tason korottamiseen. Lisäksi otsikon rakennetta on hieman yksinkertaistettu ja selkiytetty sekä uusien laajennuksien käyttö ja lisäys on tehty helpommaksi. IPv6-kehyksen rakenne on esitetty kuvassa 2-4. Yksi rivi kuvassa vastaa 32 bittiä.



Kuva 2-4: IPv6-kehyksen rakenne /9/

Osoitekenttien koon kasvattaminen 32 bitistä 128 bittiin ja osoitteistuksen osittainen uudelleenmäärittäminen on johtanut siihen, että ainoastaan noin 15 % IPv6:n osoiteavaruudesta on ennalta määrätty nykyisten IP-verkkojen perusteella. Tämä mahdollistaa verkon voimakkaan laajentamisen tarvittaessa. Nykyinen IP-osoiteavaruus on nopeasti käymässä vähiin, joten uudistus tulee tarpeeseen. /9/

2.3 Transmission Control Protocol - TCP

TCP (Transmission Control Protocol) on yhteydellinen päästä-päähän protokolla, jonka tarkoitus on taata erittäin luotettava yhteys pakettikytkentäisissä verkoissa. TCP on suunniteltu kerrostyyppiseen protokollahierarkiaan sopivaksi ja se tukee yhteyksiä usean verkon yli. Periaatteessa TCP pystyy toimimaan luotettavasti hyvin erilaisten siirtoteiden päällä aina suorista yhteyksistä piiri- tai pakettikytkentäi-

siin verkkoihin. TCP-kehyksen rakenne on esitetty kuvassa 2-5. Kuvassa yksi rivi vastaa 32 bittiä.

<table>
<tr><td colspan="3">Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgement Number</td></tr>
<tr><td>Offset</td><td>Reserved</td><td>Control</td><td>Window</td></tr>
<tr><td colspan="3">Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="3">Options</td><td>Padding</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

Kuva 2-5: TCP-kehyksen rakenne /10/

TCP-yhteys katsotaan täysin määritellyksi, kun tiedetään yhteyden osapuolien osoite (IP-osoite, kts. kuvat 2-2 ja 2-7) sekä porttinumero./3/ Näin määritellyn yhteyden sisältö voitaisiin tarvittaessa siirtää erillään muusta verkossa kulkevasta tiedosta. Liikenteen välityksen kannalta oleellisimman osan TCP-kehyksessä muodostavat kaksi ensimmäistä kenttää (Source Port ja Destination Port, 2 tavua kumpikin), jotka määrittävät yhteyden osapuolten porttinumerot. Internet-osoite ja porttinumero määrittävät yksiselitteisesti yhteyden (ns. socket) sovellustasolle asti kahden osapuolen välillä. Porttinumero voidaan yhteydenmuodostuksen aikana valita vapaasti, mutta useimmat ylempien sovellustasojen tarjoamat palvelut (pääteyhteydet, tiedostonsiirto) vaativat ennalta määrätyn porttinumeron, jotta yhteys voidaan muodostaa.

TCP on yhteydellinen protokolla, joka takaa luotettavan tiedonsiirron kahden osapuolen välillä. Perusmuotoinen yhteydenmuodostus tapahtuu nk. 3-way kättelyn avulla. Yhteys ja sen muodostus perustuu yhteyden osapuolten välillä tapahtuvaan tiedottamiseen osapuolten tilatiedoista. Taulukossa 2-1 on esitetty yksinkertaistetusti yhteydenmuodostus, jossa TCP A osapuoli aloittaa yhteydenoton TCP B:hen.

Taulukko 2-3: Yksinkertaistettu TCP-yhteyden muodostus /10/

	TCP A			TCP B
1	CLOSED			LISTEN
2	SYN-SENT	->	->	SYN RECEIVED
3	ESTABLISHED	<-	<-	SYN RECEIVED
4	ESTABLISHED	->	->	ESTABLISHED
5	ESTABLISHED+DATA-lähetys	->	->	ESTABLISHED

Varsinainen tiedonsiirto aloitetaan vasta sitten, kun vastaanottaja on siirtynyt ESTABLISHED-tilaan. Ylläolevassa taulukossa 2-1 esitetyn yhteydenmuodostustavan lisäksi TCP-yhteys voidaan muodostaa usealla muulla tavalla, jotka poikkeavat toisistaan lähinnä lähettäjän ja vastaanottajan alkutilan suhteen. Lisäksi protokolla selviää erilaisista virhetilanteista yhteydenmuodostuksen aikana.

TCP-yhteys puretaan, kun lähettäjä tai vastaanottaja pyytää yhteyden sulkemista, tai kun kumpikin osapuoli pyytää yhteyden sulkemista yht'aikaa. Yksinkertaistettu malli yhteyden sulkemisesta on esitetty taulukossa 2-2, jossa TCP A osapuoli tekee aloitteen yhteyden lopettamiseksi.

Taulukko 2-4: Yksinkertaistettu TCP-yhteyden sulkeminen /10/

	TCP A			TCP B
1	ESTABLISHED			ESTABLISHED
2	FIN-WAIT-1	->	->	CLOSE-WAIT
3	FIN-WAIT-2	<-	<-	CLOSE-WAIT
4	TIME-WAIT	<-	<-	LAST-ACK
5	TIME-WAIT	<-	<-	CLOSED
6	CLOSED			

TCP-protokollaa käytetään internet-verkoissa mm. tiedostonsiirtoon, pääteyhteyksiin, WWW-dokumenttien välitykseen, news-palvelun välittämiseen ja usean muun sellaisen palvelun yhteydessä, joita voidaan luonnehtia yhteydellisiksi. /10/

2.4 UDP - User Datagram Protocol

UDP-protokolla välittää viestejä pakettikytkentäisissä verkoissa yhteydettömästi. UDP ei takaa tiedon perillemenoa tai virheettömyyttä. UDP olettaa, että Internet-protokollaa (IP) käytetään tietopakettien lähettämiseen. Kuvassa 2-6 on esitetty UDP-kehyksen rakenne. Yksi rivi kuvassa vastaa 32 bittiä.

Source Port	Destination Port
Length	Checksum
Data octets	

Kuva 2-6: UDP-kehyksen rakenne /11/

UDP-kehys on kuin riisuttu TCP-kehys. Pakettien välittämisen kannalta tärkeimmät kentät UDP-kehyksessäkin ovat lähettäjän ja vastaanottajan porttinumeroille varattu tila. Lähettäjän porttinumeroa ei tarvitse välttämättä määritellä, jollei sillä ole vastaanottajan kannalta merkitystä. UDP-protokollaa käytetään mm. sähköpostin ja verkonhallinnan sanomien välittämiseen. /11/

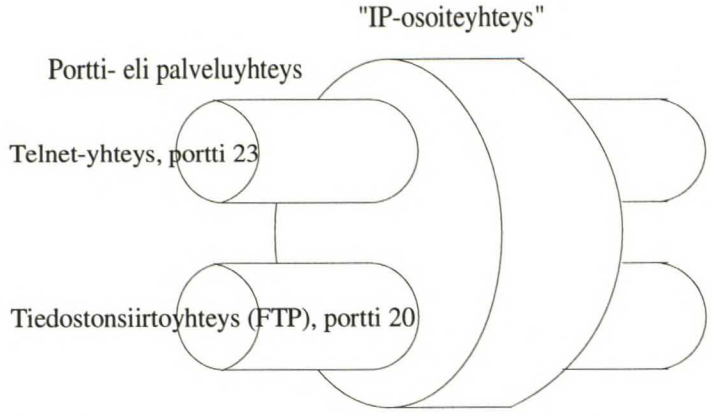
2.5 Multicast-liikenne internet-verkossa

Internet-protokollia käytettäessä multicast eli monilähetystoiminto on toteutettu ns. monilähetysosoitteiden avulla. Reitittimet ja sillat ohjaavat ja rajoittavat monilähetysviestien leviämistä, siten että nämä viestit leviävät yleensä vain yhteen aliverkkoon. Internet-verkoissa yleisesti käytössä olevat ns. jaetun median lähiverkot (Ethernet ja Token Ring) mahdollistavat kätevästi siirtotien kuuntelun ja verkon jäsenet voivat näin poimia verkosta toisaalta omaan osoitteeseensa ja toisaalta monilähetysosoitteisiin tulevat IP-paketit. /10/

2.7 Yhteenveto

Internet-protokollapino on suunniteltu tiedon välitykseen topologialtaan monimuotoisissa pakettikytkentäisissä verkoissa. Osoitteistuksen monipuolisuuden vuoksi IP-protokollien avulla voidaan välittää myös yleis/monilähetysliikennettä (broadcast ja multicast). Lisäksi internet-verkot on suunniteltu kohtuullisen hierarkisiksi, joten vika jossain verkon osassa, ns. aliverkossa, ei välttämättä vaikuta muihin verkon osiin millään lailla.

Yhteydet internet-verkoissa määritellään internet-osoitteiden ja palveluporttien avulla. Internet-osoite määrittää päätelaitteen rajapinnan sijainnin verkossa ja palveluportin numero kertoo mitä palvelua päätelaitteen toivotaan tukevan. Näin kaksi yhteyden osapuolta voivat käyttää useaa eri internet-palvelua samanaikaisesti eli kyseessä on eräänlainen palvelujen yhteensovittaminen osoiteyhteydellä. (kuva 2-7).



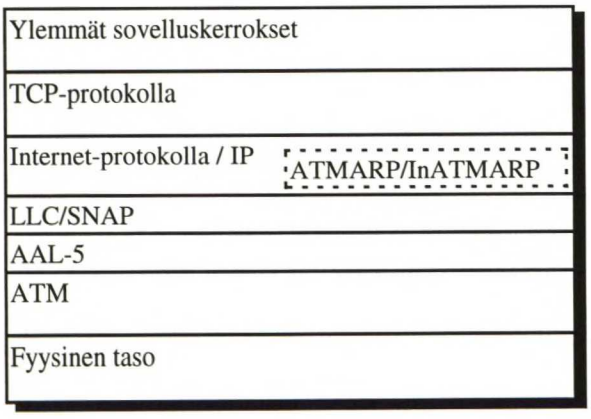
Kuva 2-7: Osoitteet ja portit TCP/IP-verkossa/looginen tarkastelu

Verrattaessa kuvaa 2-7 kuvaan 1-2 huomataan, että IP-ajattelun ja ATM-ajattelun periaatteellinen ero ei ole suuri: Kummassakin ajattelumallissa voidaan yhden suuren putken sisällä (VP tai IP-osoite) kuljettaa pienempiä samaan kohteeseen kulkevia yhteyksiä (VC tai portti). On kuitenkin huomattava, että virtuaaliväylät on tarkoitettu lukumäärältään jopa useiden satojen virtuaalikanavien reitittämisen yksinkertaistamiseen, kun taas IP-osoitteiden luomat putket pitävät sisällään parhaimmillaankin vain muutamia saman koneen eri TCP-portteihin kulkeutuvia yhteyksiä. Lisäksi välitettävän liikenteen ominaisuudet poikkeavat toisistaan tarkasteltaessa suuria ATM-runkoverkkoja ja Internet-yhteyksiä. Erityisiksi ongelmakohdiksi sovitettaessa IP-liikennettä ATM-verkkoihin muodostuvat monilähetysyhteydet ja ATM- ja IP-osoitteiden vastaavuuksien selvittäminen ja ylläpito.

3 *IP over ATM* -standardi

3.1 Yleistä

IP over ATM -standardi, joka tunnetaan myös nimellä *Classical IP over ATM*, määrittelee IP-pakettien välittämistavan ATM-verkossa, kun kyseessä on nk. IP-aliverkko, joka on yhteydessä muihin verkkoihin yhden tai useamman reitittimen välityksellä. Menetelmää voidaan hyödyntää ATM-tekniikan käyttämiseksi lähiverkoissa, paikallisissa pienissä runkoverkoissa ja IP-reitittimien välisten runkoverkkojen (kts. myös kuva 2-3) liikenteen ohjauksessa. Kuvassa 3-1 on esitetty *IP over ATM* -ratkaisuissa käytetty protokollapino.



Kuva 3-1: IP over ATM -protokollapino /12/

Kuten kuvasta 3-1 huomataan, ratkaisu on melko yksinkertainen ja suoraviivainen. Ainoat varsinaiset lisäykset jo käytössä oleviin protokolliin ovat jatkossa esiteltävät ATMARP (ATM Address Resolution Protocol)-protokolla ja tämän käänteistoiminnon suorittava InATMARP (Inverse ATM Address Resolution Protocol) -protokolla. Näitä toiminteita varten aliverkossa tulee olla vähintään yksi ATMARP-palvelin, joka toteuttaa kummaltakin protokollalta vaadittavat toiminnot. Tarvittaessa tämä palvelin voidaan integroida ATM-kytkimen tai aliverkon loogisella rajalla sijaitsevan reitittimen yhteyteen, mutta tämä luonnollisesti laskee aliverkon sisäisen toiminnan vikasietoisuutta. *IP over ATM* pystyy hyödyntämään sekä pysyviä (PVC) että signaloituja virtuaaliyhteyksiä (SVC) ja soveltuu näinollen kaikkiin ATM-ratkaisuihin. Pysyviä virtuaaliyhteyksiä käytettäessä on kuitenkin

huomattava, että *IP over ATM* -ympäristön ylläpito käy kohtuuttoman työlääksi, mikäli verkossa olevien koneiden määrä kasvaa.

3.2 LLC/SNAP ja AAL-5

Sellaisessa ATM-tekniikkaa käyttävässä verkossa, jossa siirretään useaa erilaista protokollaa, täytyy jokainen siirrettävä protokolla välittää omalla virtuaaliyhteydellään. LLC (Logical Link Control)-kapseloinnin avulla on kuitenkin mahdollistaa välittää erilaisia protokollia samalla virtuaaliyhteydellä. Eri protokollia välitettäessä lähetettävään tietoon lisätään LLC-otsikko, joka kertoo minkätyyppistä protokollaa seuraavassa tietokehyksessä käytetään. Käytettäessä protokollia, jotka eivät kuulu ISO:n (International Standardization Organization) standardoimiin täytyy LLC-kapseloinnin yhteydessä käyttää myös ns. SNAP (SubNetwork Access Point) -menettelyä./13/

Standardin /14/ mukaan *IP over ATM* -toteutusten täytyy tukea joko tiedon kapselointia IEEE 802.2 LLC/SNAP menetelmällä tai eri yhteyksien jakamista omille virtuaaliyhteyksilleen. Menetelmä valitaan yhteydenmuodostuksen yhteydessä joko manuaalisesti tai merkinannon avulla riippuen siitä käytetäänkö pysyviä tai kytkentäisiä virtuaaliyhteyksiä. Käytettäessä LLC-kapselointia IP-protokollalle täytyy AAL-5 kehyksen ensimmäisiksi tavuiksi pakata kahdeksan tavua LLC/SNAP-otsikkotietoja (kuva 3-2, kts. myös kuva 1-4). Otsikkotiedot koostuvat LLC-, OUI- ja PID-kentistä.

LLC 3 tavua	OUI 3 tavua	PID 2 tavua	Data 0- 65526 tavua	PAD	UU	CPI 1 tavu	Pituus 2 tavua	CRC-32 4 tavua

Kuva 3-2: AAL-5 CP PDU-paketin rakenne IP over ATM -yhteydellä

LLC-, OUI- ja PID-kenttien arvot ovat reititetylle IP-protokollayksikölle seuraavan taulukon 3-1 mukaiset (arvot heksadesimaalisina tavuittain):

Taulukko 3-1: LLC/SNAP-kenttien arvot IP over ATM -ympäristössä /14/

Kenttä / Siirrettävä tieto	IP PDU	ATMARP / InATMARP	Merkitys
LLC (3 tavua)	AA-AA-03	AA-AA-03	SNAP-otsikko seuraa
OUI (3 tavua)	00-00-00	00-00-00	Ethertype seuraa
PID (2 tavua)	08-00	08-06	IP PDU / ATMARP PDU

LLC-kentän arvo (AA-AA-03) määrittää, että LLC-kenttää seuraa SNAP-otsikko. SNAP-otsikon arvo (00-00-00) määrittää, että seuraavat kaksi tavua ilmaisevat Ethertype-tyyppisen protokollan. PID-kentän arvo määrittää otsikkotietoja seuraavan tiedon kuuluvan tiettyyn protokollayksikköön. Lähetettäessä ATMARP- tai InATMARP-kyselyjä PID kentän arvo on 08-06 ja IP-protokollia käytettäessä PID on 08-00. /13, 14, 15/

3.3 ATMARP ja InATMARP

ATMARP-protokolla perustuu ARP -protokollaan (Address Resolution Protocol), mutta sitä on muokattu, jotta se toimisi yhteydellisessä ATM-ympäristössä. Perusmuotoinen ARP-protokolla lähettää kaikki paketit multicast-osoitetta käyttäen. *IP over ATM* -ympäristö ei kuitenkaan tue monilähetystä standardoidusti, joten ARP-protokollaan on täytynyt tehdä tältä osin muutoksia. ATMARP palauttaa kohteen ATM-osoitteen, kun sille on annettu kohteen IP-osoite. InATMARP-protokolla vastaa perinteisissä IP-verkoissa käytössä olevaa RARP (Reverse Address Resolution Protocol) -protokollaa. InATMARP palauttaa kohteen IP- ja ATM-osoitteen, kun sille on annettu virtuaaliyhteyden tunnus (VCI). ATMARP- ja InATMARP lähettävät ja vastaanottavat seuraavan taulukon (taulukko 3-2) mukaisia sanomia.

Taulukko 3-2: ATMARP- ja InATMARP-sanomat ja niiden tehtävät /15/

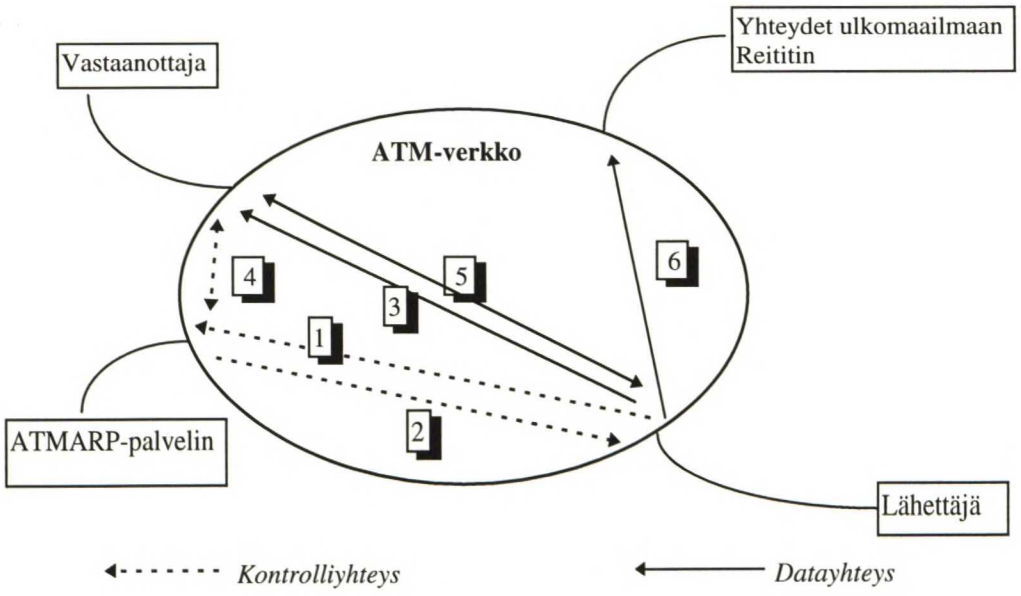
Sanoma	Tehtävä
InARP_REQUEST	Palvelimen lähettämä viesti, jonka avulla pyydetään kohdekoneen ATM- ja IP-osoite.
InARP_REPLY	Vastaus InARP_REQUEST-viestiin, jossa kohdekone kertoo oman ATM- ja IP-osoitteensa.
ARP_REQUEST	Kysely, jossa pyydetään jonkin verkossa olevan koneen IP-osoitetta vastaava ATM-osoite.
ARP_REPLY	Vastaus ARP_REQUEST-viestiin, jossa palvelin kertoo kyselyn tehneelle halutun ATM-osoitteen.
ARP_NAK	Vastaus ARP_REQUEST-viestiin, mikäli palvelimen osoitetietokannasta ei ole löytynyt haluttua vastausta.

Mikäli *IP over ATM* -verkko on toteutettu pelkästään pysyvien virtuaaliyhteyksien (PVC) avulla täytyy jokaisen aliverkossa olevan koneen tukea InATMARP-protokollaa. InATMARP-protokollaa käytetään tässä tapauksessa päättelemään, mikä verkon jäsen on kunkin virtuaaliyhteyden kautta kytkettynä. Käytettäessä kytkettyjä virtuaaliyhteyksiä (SVC) täytyy jokaisessa loogisessa aliverkossa olla ATMARP-palvelin. Palvelin ylläpitää palvelemansa verkon osoitetietokantoja sekä IP- ja ATM-osoitteiden vastaavuuksia. Palvelimen avulla verkon muut koneet voivat myös rekisteröidä verkon osoiteavaruutta omien tarpeidensa mukaan. /15/

3.4 Toiminta

Menetelmän perusajatuksena on selvittää IP-osoitteen perusteella ATM-osoite ja kytkeä yhteys näiden tietojen perusteella, tai mikäli käytetään pysyviä kytkentäisiä yhteyksiä (PVC), ohjata kaikki tiettyihin IP-osoitteisiin kulkeva liikenne tälle varatulle yhteydelle. IP-osoitteen ja ATM-osoitteen välisen muunnoksen hoitaa ATM-verkossa oleva ATMARP-palvelin. Suurin lähetettävän tietoyksikön koko (Maximum Transfer Unit, MTU) voidaan neuvotella standardoidusta 9180 tavusta aina 65536 tavuun (AAL-5 sovitustason suurin mahdollinen tietokuorma) asti. Koko aliverkossa täytyy MTU:n arvon olla sama. Suurimman lähetysyksikön koko pyritään sopimaan mahdollisimman suureksi, sillä se parantaa *IP over ATM* -ver-

kon tehokkuutta /3/. Kuvassa 3-3 on esitetty kytkentäisessä ATM-verkossa esiintyvät komponentit sekä kuvattu näiden välittämien tietovirtojen suunta ja järjestys.



Kuva 3-3: IP over ATM -verkon komponentit ja toiminta

Kun yhteyden aloittava osapuoli (lähettäjä) haluaa lähettää johonkin IP-osoitteeseen tietoa, se aloittaa yhteyden muodostamisen lähettämällä ATMARP-palvelimelle ennalta määritellyllä yhteydellä pyynnön, jossa pyydetään kohdekoneen ATM-osoitetta. Tapahtuma on esitetty kuvassa 3-3 kohdassa 1. ATMARP-palvelin vastaa pyyntöön asianmukaisella osoitteella (kuva 3-3, kohta 2), jos se löytää kohdekoneelle ATM-osoitteen, muussa tapauksessa palautetaan ATM_NAK-vastaus ja yhteydenmuodostus peruutetaan tai aloitetaan lähetys ennalta määritellyllä yhteydellä reitittimelle (kuva 3-3, kohta 6). Mikäli IP-osoite on löytynyt muodostetaan ATM-yhteys tähän osoitteeseen ja aloitetaan lähetys (kuva 3-3, kohta 3). Vastaanottajan saadessa ensimmäisen paketin, se lähettää ATMARP-palvelimelle tiedustelun lähettäjän osoitteesta ja saatuaan vastauksen (kuva 3-3, kohta 4) ja lähettäjän osoitteen voi tiedonsiirto alkaa (kuva 3-3, kohta 5). ATMARP-palvelin pitää yllä tietokantaa, jossa on tieto olemassaolevista yhteyksistä ja verkkoon liikennettä viimeeksi tuottaneiden verkon jäsenten ATM- ja IP-osoitteet. SVC-ympäristössä yhteyden muodostus tapahtuu merkinantoprotokollien (UNI 3.1 tai Q.2931) avulla /16/. Yhteys puretaan niinikään merkinannon avulla siten, että verkonhallinta tarkkailee aikavalvonnan avulla yhteyksiä, ja jos niillä ei esiinny liikennettä niin yhteys puretaan. Koska aikavalvonta tapahtuu noin 15-20 minuutin

välein, sitoo tämä verkkoresursseja. Lisäksi on mahdollisuus tarkkailla TCP-paketteja ja purkaa yhteys TCP-yhteyttä purettaessa (kts. myös taulukko 2-2). /3, 15, 17/

3.4.1 Verkon jäsenten liittyminen verkkoon

Kun verkkoon haluava kone ensimmäisen kerran ottaa yhteyden verkkoon, se ilmoittaa itsestään ATMARP-palvelimeen ennaltamäärätyllä ATM-yhteydellä, jolloin ATMARP-palvelin saa tietää koneen ATM-osoitteen. ATMARP-lähettää InATMARP-pyynnön ja pyytää ko. koneen IP-osoitetta. ATMARP-palvelin kysyy säännöllisin väliajoin verkossa olevien koneiden ATM ja IP-osoitteita ja ylläpitää tietoja verkon ATM- ja IP-osoitteiden vastaavuuksista. Mikäli jokin kone ei vastaa osoitetiedusteluihin, ATMARP-palvelin poistaa tämän tiedot muististaan. Tarkoitus on optimoida ATMARP-taulukoiden kokoa ja nopeuttaa palvelimen toimintaa. Tulevaisuudessa on tarkoitus standardoida toimintamuoto, jossa palvelin oppisi ylläpitämään koneiden osoitetietoja tarkkailemalla verkossa esiintyvää liikennettä. Myös verkon jäsenet voivat pitää yllä omia osoitetaulukoitaan. /3, 10, 17/

3.4.2 Monilähetysliikenne *IP over ATM* -ympäristössä

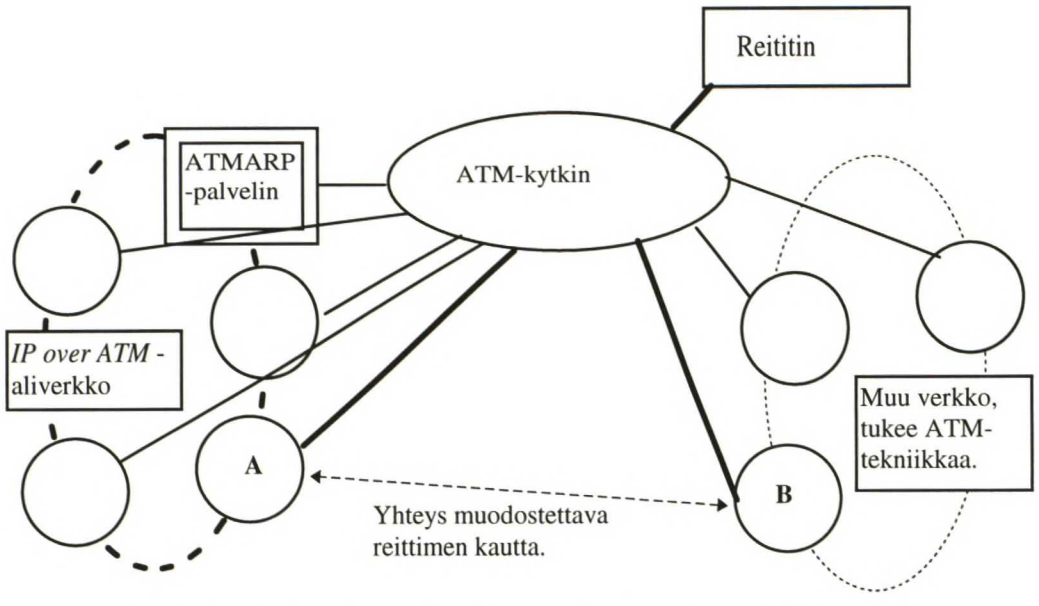
Monilähetystoiminnetta ei ole määritelty *IP over ATM* -standardeissa. Standardeissa mainitaan muutama ehdotus monilähetystoiminteen toteuttamiseksi, mutta lopulliset käytännön toteutukset ovat kuitenkin aliverkkokohtaisia. Mikäli halutaisiin lähettää yleislähetysviestejä (broadcast), eli viestejä kaikille aliverkossa oleville, täytyisi jokainen paketti monistaa ja lähettää se erikseen halutuille (kaikille) aliverkossa oleville koneille. Multicast-viestejä, eli viestejä rajatulle joukolle, voitaisiin tarvittaessa lähettää myös erityisen monilähetyspalvelimen kautta. Monilähetyspalvelimen toiminta voitaisiin integroida ATMARP-palvelimen yhteyteen ja siihen otettaisiin yhteys aina, kun halutaan lähettää monilähetysviestejä. /3, 10, 17/

3.5 Yhteenveto

IP over ATM -ratkaisu tarjoaa hyvin yksinkertaisen ja toimivan, joskin eräiltä osin rajoittuneen palvelun ATM-tekniikan käyttämiseksi IP-ympäristöissä. Toimivia tuotteita on markkinoilla ja verkkoympäristö on helposti perustettavissa.

IP over ATM -ratkaisun päällimmäisenä heikkoutena on monilähetystoiminteen toteutuksen puute. Heikkoutena on myös huono sietokyky aliverkon muutoksille: ATMARP-palvelimen ATM-osoite täytyy määrittää käsin jokaiselle verkon jäsenelle. ATMARP-palvelin muodostaa *IP over ATM* -verkossa pullonkaulan ja saattaa mahdollisesti estää koko aliverkon toiminnan, mikäli sen toiminta häiriintyy tai lakkaa kokonaan. Kehitteillä on järjestelmä, jossa em. osoite saadaan suoraan verkosta, esimerkiksi merkinantokanavan kautta, jolloin palvelimen toiminnot voidaan toistaa verkossa helpommin.

IP over ATM -verkon koneet eivät voi olla samanaikaisesti jonkin toisen IP-aliverkon jäseniä. Tämä tarkoittaa sitä, että yhteys joudutaan luomaan määritellyn aliverkon ulkopuolelle reitittimen kautta, vaikka suora ATM-yhteyskin olisi mahdollinen (kuva 3-4).



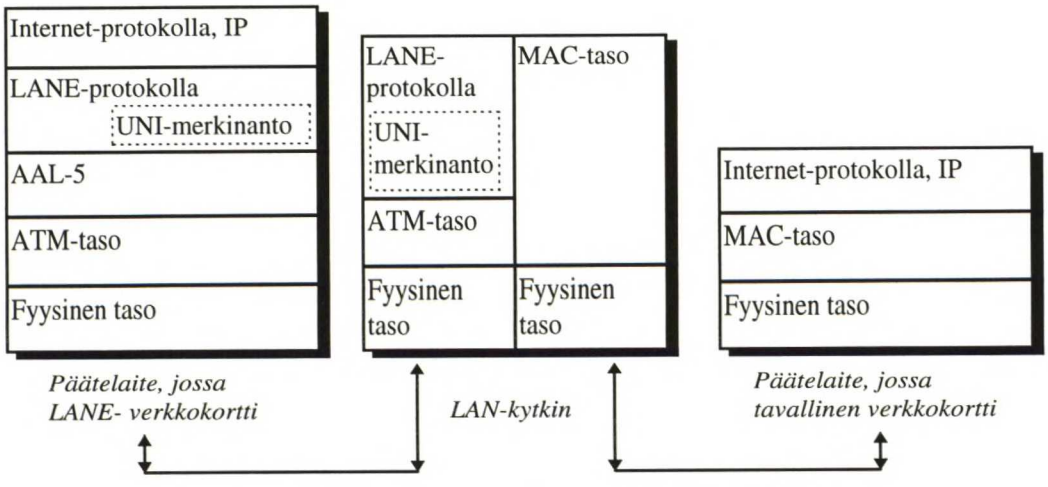
Kuva 3-4: Aliverkon yhteydenmuodostus verkon ulkopuolelle

IP over ATM -ratkaisu ei tue erillisiä ylemmistä tasoista riippuvaa palveluluokkien määritystä aliverkossa. Aliverkon kaikille yhteyksille voidaan määrittää yksi yhteinen palveluluokka, mutta tämä johtaa väistämättä kompromisseihin käyttäjän kokemaan palvelun laadun ja verkkoresurssien optimaalisen käytön välillä.

4 ATM Forumin lähiverkkoemulaatio

4.1 Yleistä

Lähiverkolla tarkoitetaan seuraavassa sellaisia tietoliikenneratkaisuja, jotka rajoittuvat maantieteellisesti hyvin pienelle alueelle (rakennus tai rakennuksen yksittäinen kerros), joissa siirtotie on loogisesti jaettu kaikkien verkon jäsenien kesken ja joissa siirtotien käyttöä kontrolloidaan erityisten menetelmien avulla /4/. ATM Forumin määrittelemä lähiverkkoemulaatio (Local Area Network Emulation, LANE) tarjoaa lähiverkkokytkinten ja reitittimien avulla ylemmille protokollakerroksille virtuaalisen lähiverkko-palvelun. Lähiverkkoemulaatio on toistaiseksi standardoitu kahdelle perinteiselle lähiverkkotekniikalle IEEE 802.3 Ethernetille ja IEEE 802.5 Token Ringille. Alemmille protokollakerroksille emuloitu lähiverkko (ELAN) tarjoaa normaalin ATM-rajapinnan. LANE-protokolla määrittelee perinteistä lähiverkkoa vastaavan rajapinnan ylemmän tason protokollille ja tieto kuljetetaan ATM-verkossa normaalissa LAN MAC-paketissa. Kuitenkaan varsinaista perinteisille lähiverkoille tyypillistä siirtotien valvontaa ja sille pääsyn kontrollointia (Ethernetissä CSMA/CD ja Token Ringissä valtuuspaketin välittämistä) ei toteuteta. LANE:n avulla lähiverkko toimii kuten silloitettu verkko. Siltana (bridge) toimii tällöin erityinen lähiverkkokytkin. Kuvassa 4-1 on protokollapinojen avulla esitetty LANE:n mukaisesti toteutetun lähiverkon toimintamalli.



Kuva 4-1: LAN-emulaation protokollamalli /18/

Verkossa voi periaatteessa olla sekä emuloitavaa lähiverkkoa käyttäviä päätelaitteita että lähiverkkoemulaatiota tukevia päätelaitteita. LANE-protokollan avulla voidaan yhden fyysiseen siirtomedian piirissä olevaan ympäristöön määrittää useita loogisesti erillisiä lähiverkkoja. /3, 17/

4.2 Lähiverkkoemulaation loogiset rakenneosat

Lähiverkkoemulaation avulla toteutettu lähiverkko sisältää useita loogisia komponentteja, jotka esitellään seuraavassa (kts. myös kuva 4-2):

Lähiverkkoemulaatio-asiakas (LAN Emulation Client, LEC) esiintyy jokaisessa päätelaitteessa. Jokaista emuloitua lähiverkkoa kohden, johon päätelaite kuuluu, on päätelaitteessa yksi erillinen LEC. Lähiverkkoemulaatio-asiakas tarjoaa sovellustason protokollille emuloitavan LAN-standardin mukaisen rajapinnan. LEC identifioidaan ATM-osoitteella, joka on sidottu yhteen tai useampaan MAC-tason osoitteeseen. Esimerkiksi yhden LAN-kytkimen ATM-osoite on sidottu kaikkiin niihin MAC-tason osoitteisiin, joihin sillä on yhteys. Lisäksi lähiverkkoemulaatio-asiakas huolehtii tiedon lähetyksestä, osoitepalveluista ja muista kontrollifunktioista.

Lähiverkkoemulaatio-palvelin (LAN Emulation Server, LES) toteuttaa emuloidun lähiverkon hallintafunktiot. Jokaista emuloitua lähiverkkoa kohden tulee olla vain yksi looginen LES. Lähiverkkoemulaatio-palvelin on identifioitu yksilöllisellä ATM-osoitteella ja mikäli päätelaite haluaa käyttää emuloidun lähiverkon palveluja täytyy päätelaitteen olla yhteydessä ao. lähiverkon LES:iin.

Monilähetyspalvelin (Broadcast and Unknown Server, BUS) ohjaa multicast-viestit ja tuntemattomiin osoitteisiin osoitetut viestit kaikille emuloidun lähiverkon jäsenille. Monilähetyspalvelin identifioidaan ATM-osoitteella, joka on lähiverkkoemulaatio-palvelimessa määritelty sellaiseksi MAC-osoitteeksi, johon lähetetään yleis- ja monilähetysviestit.

Emuloidun lähiverkon konfigurointipalvelin (LAN emulation Configuration Server, LECS) ohjaa jokaisen lähiverkkoemulaatio-asiakkaan oikealle lähiverkkoemulaatio-palvelimelle. ATM-aliverkossa on vain yksi looginen LECS, joka palvelee kaikkia emuloituja lähiverkkoja tässä verkkosegmentissä (vrt. IP-aliverkot).

Edellä esiteltyjen palvelinkomponenttien toiminnot voidaan toteuttaa yhdessä lait-

teessa, mutta verkon vikasietoisuuden parantamiseksi pyritään toimintoja yleensä hajauttamaan.

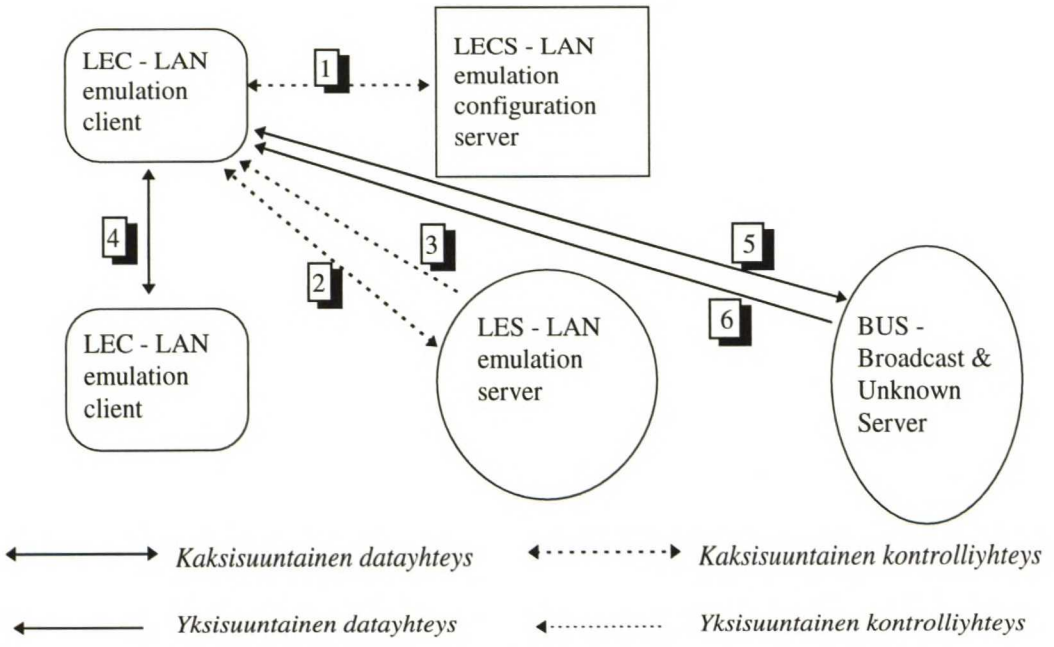
ATM Forumin lähiverkkoemulaation versiossa 1.0 on määritelty vain emuloidun lähiverkon asiakas-palvelin rajapinta (LEC-LES rajapinta, LUNI). Seuraavaan versioon lähiverkkoemulaation määrittelystä aiotaan sisällyttää myös useamman LES:in, LECS:in ja useamman BUS:in väliset rajapinnat (LAN emulation network to network interface, LNNI). /17,18/

4.2.1 Lähiverkkoemulaation fyysiset rakenneosat

Emuloitu lähiverkko koostuu fyysisesti lähinnä kahdenlaisista komponenteista. ATM-päätelaitekortit toteuttavat LANE-protokollan ja toimivat rajapintana ATM-verkkoon. Toisaalta ne tarjoavat sovelluksille perinteisen lähiverkon kaltaisen palvelun. Sovellusten verkkoprotokollat olettavat olevansa tekemisissä tavallisen lähiverkon kanssa. Toinen komponenttiryhmä ovat ATM-verkkoon liitetyt LAN-kytkimet ja reitittimet. LAN-kytkimen eri portit voidaan määritellä kuulumaan loogisesti eri lähiverkkoihin ja näin ne tarjoavat ns. virtuaalisen lähiverkkopalvelun. Nykyisissä LAN-kytkimissä on toteutettu myös kaikki edellisessä kohdassa esitetyt palvelimet. /17, 18/

4.3 Emuloidun lähiverkon toiminta

LAN emuloidussa verkossa esiintyvät virtuaaliyhteydet jakautuvat kontrolli- ja datayhteyksiin. Kontrolliyhteyksillä siirretään emuloidun lähiverkon toiminnan ja hallinnan kannalta välttämätöntä tietoa ja datayhteyksillä tapahtuu verkon asiakkaiden välinen tiedonsiirto. Kuvassa 4-2 on esitetty emuloidun lähiverkon komponentit sekä näiden välille muodostettavat yhteydet.



Kuva 4-2: LAN-emulaatio komponentit ja yhteydet /17, 18/

Emuloidun lähiverkon toiminta voidaan karkeasti jakaa kolmeen osaan: 1) alustus ja konfigurointi, 2) liittyminen ja rekisteröityminen, 3) osoitteiden selvittäminen ja tiedonsiirto. Asiakkaan (LEC) liittyessä verkkoon, se ottaa yhteyden konfigurointi-palvelimeen (LECS) ja saa palvelimelta tarvitsemansa tiedot, jotta se voi liittyä haluamaansa lähiverkkoon. Tapahtuma on esitetty kuvassa 4-2 kohdassa 1. Tämän jälkeen asiakas ottaa yhteyden LANE-palvelimieen (LES) ja muodostaa kaksi erillistä kontrolliyhteyttä palvelimeen. Näiden yhteyksien kautta välitetään muun muassa osoiteinformaatiota muista verkossa olevista asiakkaista (kuva 4-2, kohdat 2 ja 3). Asiakas muodostaa datayhteyksiä toisiin verkon asiakkaisiin ja monilähetys-palvelimeen (BUS). Näiden yhteyksien avulla asiakas hoitaa tiedon lähetyksen muille asiakkaille (kuva 4-2 kohta 4) tai monilähetyspalvelimeen (kuva 4-2, kohta 5) ja vastaanoton asiakkailta tai monilähetyspalvelimelta (kuva 4-2, kohdat 4 ja 6). Eri yhteystyypit ja niiden liittyminen emuloidun lähiverkon toimintaan on esitetty taulukossa 4-1. /17,18/

Taulukko 4-1: Lähiverkkoemulaatiossa esiintyvät yhteystyypit /17, 18/

Tapahtuma	Yhteystyyppi
Verkkoon liittyminen	Configuration Direct VCC
Osoitteiden selvitys	Control Direct VCC
Verkon muut asiakkaiden selvitys	Control Distribute VCC
Tiedon lähetys yksittäiselle verkon jäsenelle	Data Direct VCC
Tiedon lähetys usealle verkon jäsenelle	Multicast Send VCC
Multicast lähetysten vastaanotto	Multicast forward VCC

4.3.1 Multicast-liikenne emuloidussa lähiverkkoympäristössä

Lähiverkkoemulaatiossa monilähetystoiminne on toteutettu erityisen multicast-palvelimen (BUS) avulla. Lähetettäessä useille vastaanottajille IP-paketteja lähetetään nämä paketit ensin multicast-palvelimelle, joka toimittaa paketit edelleen kaikille vastaanottajille. Menetelmä on melko raskas ja kuormittaa verkon resursseja sekä uusien yhteyksien muodostuksen että tiedon monistumisen takia. /18/

4.4 Yhteenveto

Lähiverkkoemulaatio on nykyään melko laajalti tuettu teknologia, joka käyttää hyväksi ATM-teknologiaa tiedonsiirrossa. Menetelmän avulla tarjotaan jo käytössä olevien lähiverkkoteknologioiden palveluita, nyt kuitenkin uudella fyysisellä siirtokerroksella.

Lähiverkkoemulaation selkein etu on se, että verkossa voi olla sekä LANE-palvelimeen liittyneitä jäseniä että tavallista lähiverkkotekniikkaa käyttäviä asiakkaita. Tämä on mahdollista, koska LAN-kytkimet tunnistavat myös perinteisiä lähiverkkotekniikoita käyttävät päätelaitekortit. Näin ollen siirtyminen ATM-tekniikkaan käy asteittain ja kohtuullisen huomaamattomasti.

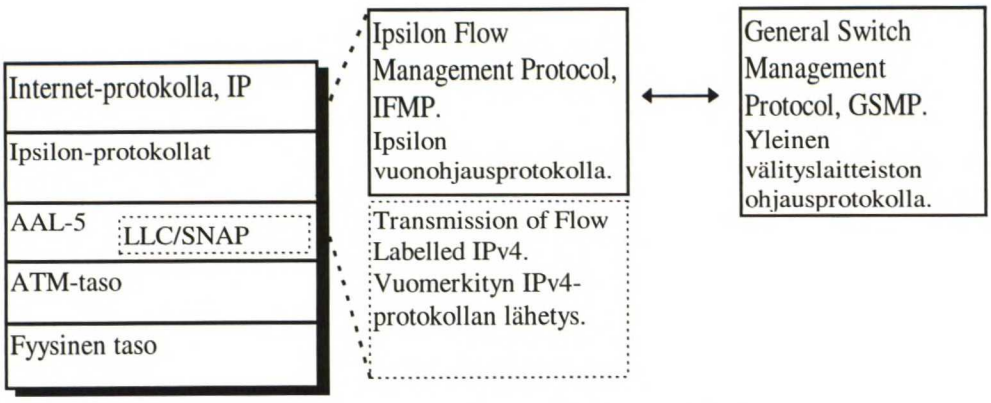
Selkeänä haittapuolena on protokollapinon toiminteiden toteuttamisen aiheuttama kuormitus verkolle ja siihen liitetyille komponenteille. Yhteyksien muodostus signaloinnin avulla kuormittaa verkkoa eikä palvelun tasoa pystytä takaamaan. Käytännössä kaikki yhteydet ovat palveluluokaltaan ABR- tai UBR-tyyppisiä ATM-yhteyksiä. Toisaalta tämäntyyppisten palveluluokkien toteutus emuloi erittäin hyvin perinteisten lähiverkkoratkaisujen palvelutasoa.

Lähiverkkoemulaatio on saavuttanut kohtuullisen kaupallisen suosion, kun lähiverkkoihin on etsitty suorituskyvyn parannusta, mutta ei olla haluttu tai ei ole ollut resursseja siirtyä kokonaan uudenlaisen teknologian käyttöön. Lähiverkkoemulaation käyttöönoton yhteydessä fyysiset tiedonsiirtonopeudet yleensä kasvavat (esimerkiksi 10 Mbps -> 25 Mbps), mutta ratkaisun edellämainitun raskauden takia varsinainen suorituskyvyn parantuminen on yleensä pienempi.

5 IP-kytkentä

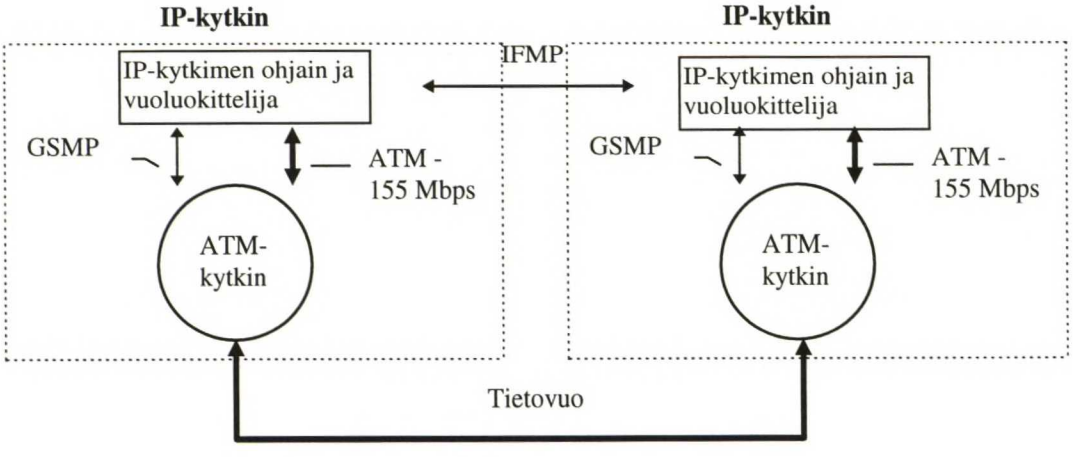
5.1 Yleistä

Internet-verkoissa välitettävä liikenne on useassa tapauksessa luonteeltaan yhteydellistä, vaikka itse liikenteen välitys tapahtuukin IP-protokollan avulla yhteydettömästi. IP-pakettien virrasta tietoliikenneverkkojen solmukohdissa voidaan kuitenkin erotella sellaiset pienemmät pakettivirrat, IP-vuot, joiden lähettäjä ja vastaanottaja ovat samat. Tuntuisi järkevältä pyrkiä ohjaamaan tämänkaltaiset IP-vuot omille ATM-yhteyksilleen. Toisaalta tällöin lyhytaikaiset yhteydelliset ja yhteydettömät internet-verkon palvelut kuormittaisivat verkkoa ja yhteydenmuodostuksen komponentteja tarpeettomasti. Tähän ongelmaan on esitetty ratkaisuksi vain pitkäikäisten ja paljon tietoa siirtävien IP-voiden kytkemistä omille ATM-yhteyksilleen heti reitityspäätösten tekemisen jälkeen. Eräs ratkaisu tähän ongelmaan, nyt jo markkinoiltakin saatavissa oleva, on esitetty USA:laisen Ipsilon Inc. yhtiön toimesta. Yrityksen kehittämä Ipsilon-järjestelmä on kaikilta olennaisilta osin standardoitu ja standardit ovat julkisesti saatavilla. Ipsilon-järjestelmä koostuu tavallisesta IP-reitittimestä ja ATM-kytkimestä, jotka on integroitu yhdeksi laitteeksi. Järjestelmän tarkoituksena on pienentää reitittimissä IP-pakettien käsittelyssä syntyviä viiveitä ja näin tehostaa verkon suorituskykyä. Järjestelmän avulla voidaan tiettyjä IP-voita kytkeä suoraan ATM-tasolla, ilman että pitäisi tutkia jokaisen IP-paketin otsikkotietoja reitityspäätösten tekemiseksi. Käytännössä vain sellaiset IP-vuot, joissa kulkee paljon siirrettävää tietoa tai joissa yhteysajat ovat pitkiä, kytketään suoraan ATM-tasolla ja loput reitite tään kuten tavallisissa reitittimissä. Yhteyden luominen jokaista IP-vuota varten kuormittaisi ATM-verkkoa tarpeettomasti ja tuottaisi tarpeetonta viivettä muulle liikenteelle. Ratkaisussa käytettävät protokollat ja niiden asema Ipsilon-järjestelmässä sekä protokollien suhde muihin verkossa käytettyihin protokolliin on esitetty kuvassa 5-1.



Kuva 5-1: Ipsilon-protokollahierarkia

Protokollarakenteesta huomataan, että kaikki ATM-spesifiset korkeamman tason protokollat (signalointi, reititys, LES, ARP) on poistettu AAL-5 tason jälkeen ja tilalle on sijoitettu vuonohjausprotokolla (IFMP), jonka avulla ohjataan omille virtuaaliyhteyksilleen sopivat IP-vuot ATM-yhteyksille. Erikseen on määritelty ATM-välityslaitteistoa ohjaava ja valvova protokolla (GSMP). Lisäksi on määritelty vuoluokittelija, joka päättää pyydetäänkö lähettäjää ohjaamaan vuo omalle ATM-yhteydelleen vai tehdäänkö reitityspäätös IP-tasolla. Verkon elementtien kannalta katsottuna GSMP-protokolla kommunikoi ainoastaan yhden paikallisen ATM-välityslaitteiston kanssa, eikä sen toiminta aiheuta liikennettä tämän välityslaitteiston ulkopuolelle. IFMP-protokolla puolestaan kommunikoi verkossa sijaitsevien viereisten verkkoelementtien kanssa ja esittää välityslaitteistoille pyyntöjä ohjata tietovoita omille virtuaaliyhteyksilleen (kuva 5-2).



Kuva 5-2: Ipsilon-ympäristön periaatteellinen rakenne /19/

Yhteyksien eli tietovoiden luokittelu pitkäikäisiin ja paljon tiedonsiirtoa sisältäviksi perustuu IP-osoitteisiin ja porttinumeroihin sekä ennalta määriteltyihin oletuksiin tietyntyppisten IP-osoite/portti-kombinaatioiden liikenteen ominaisuuksista. Luvussa 6 käsitellään tarkemmin liikennemittauksia ja niiden tuloksia, joihin tällaiset oletukset liikenteestä perustuvat. Periaatteessa suurin osa (50-90 %) yhteydellistä TCP-protokollaa käyttävistä tietovoista täyttää suoralle kytkemiselle asetettavat edellytykset. Samaa periaatetta voidaan soveltaa myös eräisiin yhteydetöntä UDP-protokollaa käyttäviin sovelluksiin. /19,20/

5.1.1 Tietovuo

Ipsilon-protokollat perustuvat pitkälti ns. tietovuohon ja sellaisen tunnistamiseen. Tietovuoksi ymmärretään tässä työssä pitkäaikainen internet-protokollien avulla muodostettu pakettivirta, eli sarja internet-protokollan mukaisia paketteja, jotka on lähettänyt tietty lähettäjä (source) tietylle vastaanottajalle (destination). Pakettien otsikoissa määritellyt tiedot ovat tietyiltä osin paketista toiseen identtisiä. Tietovuo on siis yhteys, jolla kulkee tietoa tietystä lähteestä tiettyyn kohteeseen tai kohteisiin, ja johon tulee soveltaa samoja toimenpiteitä reitityksen, resurssien varaamisen ja muun vastaavan käsittelyn suhteen. Tietovuo määritetään TCP-kehyksen porttinumeroiden ja IP-kehyksen internet-osoitteiden sekä tulevaisuudessa IPv6:n tullessa käyttöön erityisen vuokentän avulla. Tietovuon käsite ei rajoitu, eikä sitä pidä rajoittaa, pelkästään yhteydellisten (TCP) protokollien käyttöön, vaan sitä tulee soveltaa tarpeen vaatiessa myös yhteydettömien protokollien välityksessä. /19, 20, 21, 22/

5.2 Vuonohjausprotokolla - IFMP

5.2.1 Yleistä

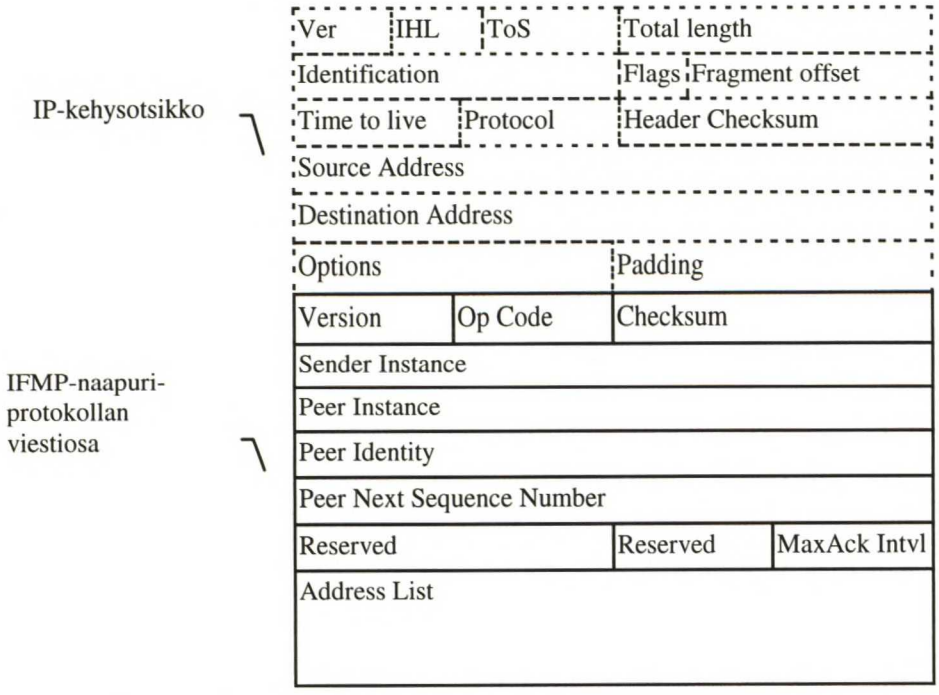
Ipsilon-järjestelmän vuonohjausprotokolla (Ipsilon Flow Management Protocol, IFMP) antaa verkossa olevalle solmulle tai muulle verkkoelementille mahdollisuuden pyytää toista verkon solmua tai muuta verkkoelementtiä muokkaamaan tietovuon IP-kehystietoja ja lisäämään ohjausinformaatiota tietovuon kehystietojen mukaan. Tämän ohjausinformaation avulla voidaan IP-tietovuot kytkeä suoraan omille virtuaaliyhteyksilleen sen sijaan, että täytyisi tehdä reitityspäätös jokaiselle IP-paketille erikseen. IFMP-protokolla tukee useita erilaisia tietovuotyyppejä ja

nykyinen versio määrittää oletustavan lisäksi kolme erilaista tietovuotyyppiä (taulukko 5-3).

IFMP-protokolla jakaantuu kahteen osaan: IFMP-naapuriprotokollaan (IFMP Adjacency Protocol), joka toimii lähinnä informatiivisena ja kontrolliyhteyden muodostavana osana IFMP-protokollaa. Naapuriprotokollalla ei ole toiminnallista funktiota liikenteen reitityksessä, se ainoastaan omilla toiminnoillaan mahdollistaa kytkentäpyyntöjen esittämisen naapurielementeille. Toinen protokolla, IFMP-ohjausprotokolla (IFMP Redirection Protocol), on Ipsilon-konseptin toiminnallinen ydin, joka pyytää lähettävän verkkoelementin ohjaamaan havaitut ja kytkemiskelpoiset IP-tietovuot omille virtuaaliyhteyksilleen. /23/

5.2.2 IFMP-naapuriprotokolla

IFMP-naapuriprotokolla mahdollistaa verkkoelementille, yleensä IP-kytkimelle, mahdollisuuden selvittää verkossa olevan loogisesti viereisen elementin identiteetin. Lisäksi protokollaa käytetään yhteyden osapuolten välisten tilojen synkronointiin, tunnistamaan yhteyden toisen osapuolen vaihtuminen ja IP-osoiteinformaation vaihtamiseen. Kaikki IFMP-naapuriprotokollaan kuuluvat viestit pakataan IPv4-kehykseen ja ne lähetetään rajoitetun lähetyksen IP-monilähetysosoitteeseen (IP-osoite 255.255.255.255). IP-otsikon protokolla-kentässä käytetään arvoa 101 (desimaali) ilmaisemaan, että kyseessä ei ole mikään muu standardoitu protokolla, ja lisäksi TTL-kentän arvolla yksi varmistetaan ettei viesti etene verkossa. IFMP-naapuriprotokollan viestin rakenne on esitetty kuvassa 5-2. Yksi rivi kuvassa vastaa 32 bittiä.



Kuva 5-3: IFMP-naapuriprotokollan viestin rakenne /23/

Version-kentässä ilmoitetaan käytettävän IFMP-protokollan versionumero.
Op Code -kenttä määrittää yksiselitteisesti viestin aiheuttaman toiminnan. Taulukossa 5-1 on esitetty Op Code -kentän arvot ja niitä vastaavat toiminnot.

Taulukko 5-1: IFMP- naapuriprotokollaviestin OpCode -kentän eri arvot /23/

OpCode	Toiminto
0	SYN, synkronointipyyntö.
1	SYNACK, synkronointipyynnön kuittaus.
2	RSTACK, kuittauksen uusinta.
3	ACK, kuittaus.

Taulukon 5-1 perusteella voidaan havaita, että IFMP-naapuriprotokolla muodostaa yhteyksiä verkossa oleviin viereisiin elementteihin paljolti samoin menetelmin kuin TCP-protokolla. Tällaisten tilatietojen avulla muodostetut ja ylläpidetyt yhteydet takaavat verkon kapasiteetin tehokkaan käytön, mutta toisaalta verkon perustoiminnan kannalta tilatietojen avulla muodostetuilla yhteyksillä ei ole ratkaisevaa merkitystä.
Checksum-kenttään lasketaan IP-kehyksen ja IFMP-naapuriprotokollan viestin tarkistussumma.

Sender Instance - ja Peer Instance -kentät ilmaisevat lähettäjän ja vastaanottajan identiteetin. Näiden kenttien arvot ovat yksiselitteisiä lähimenneisyydessä ja kentät saavat uudet arvot aina, kun kyseessä oleva laite liittyy uudestaan verkkoon.

Peer Identity -kentässä lähetetään lähettäjän olettamus vastaanottajan IP-osoitteesta. Mikäli IP-osoitetta ei tunneta kenttä saa arvon nolla.

Peer Next Sequence Number -kentässä ilmaistaan seuraavan odotetun IFMP-ohjausviestin Sequence Number -kentän arvon.

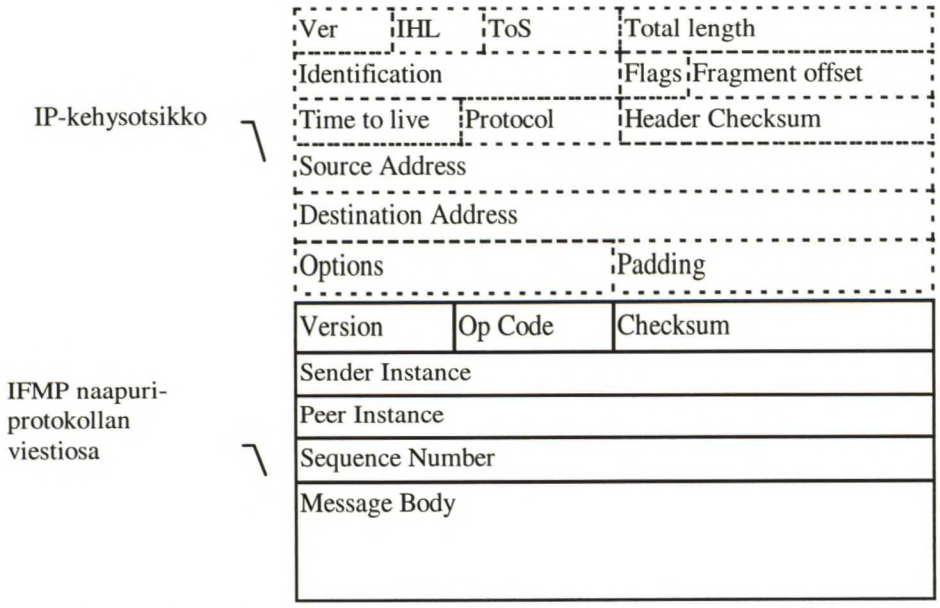
Max Ack Intvl -kentän arvo ilmaisee suurimman ajan, jonka viestin lähettäjä odottaa ennen kuin se lähettää ACK-viestin (taulukko 5-1).

Address List -kentässä lähetetään vähintään yksi IP-osoite, johon lähettäjällä on yhteys. Näitä tietoja IFMP-protokolla ei käytä, mutta niitä voidaan antaa reititysprotokollien käyttöön.

Reserved-kentät on varattu tulevaa käyttöä varten./23/

5.2.3 IFMP-ohjausprotokolla

IFMP-ohjausprotokolla muodostaa IP-kytkentätoiminnon ytimen Ipsilon-ympäristössä. Ohjausviesti (redirect-viesti) pyytää yhteyden lähettävää osapuolta muuttamaan vuolla esiintyvän liikenteen esitystapaa ja ohjaamaan tietovuon omalle virtuaaliyhteydelleen. Ohjausprotokolla mahdollistaa lisäksi käytössä olevien yhteyksien purkamisen ja virhetilanteiden havainnoimisen. Ohjausprotokollan viesti liitetään IP-kehykseen kuten naapuriprotokollankin viesti. IFMP-ohjausprotokollan viestin rakenne on esitetty kuvassa 5-4. Yksi rivi kuvassa vastaa 32 bittiä.



Kuva 5-4: IFMP-ohjausprotokollan viestin perusrakenne /23/

Version-kenttä ilmaisee käytettävän IFMP-protokollan versionumeron.

OpCode -kenttä määrittää viestin aiheuttamat toiminnot.

Ohjausprotokollan OpCode -kentän arvot, eri toiminnot ja käytetyt viestityypit on esitetty taulukossa 5-2.

Taulukko 5-2: IFMP-ohjausprotokollan toiminnot ja viestityypit /23/

OpCode-arvo	Toiminto	Viestityyppi
4	Vuon/yhteyden muodostaminen	Redirect-viesti
5	Vuon/yhteyden vapautus	Reclaim- viesti
6	Vuon/yhteyden vapautuksen kuittaus	Reclaim Ack -viesti
7	Sopimattomien arvojen ilmaisu	Label Range-viesti
8	Virheilmoitus	Virhe-viesti

Checksum-, Sender Instance - ja Peer Instance - kentät saavat vastaavan arvon, kuin IFMP-naapuriprotokollaviestissä.

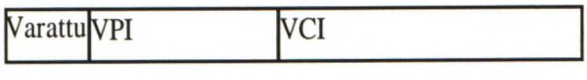
Sequence Number -kentässä lähetetään viestin järjestysnumero, joka kasvaa yhdellä aina, kun uusi viesti lähetetään. Tämän avulla vastaanottajan on mahdollista käsitellä IFMP-ohjausprotokollan viestit lähetysjärjestyksessä.

Viestityypin (taulukko 5-2) mukaan viestin MessageBody -osassa esitetään toiminnon kannalta oleellinen informaatio. Vuon hallintaan liittyvien viestien yhteydessä viestissä lähetetään aina vuotunnus ja vuotyypin tunniste. /23/

5.2.4 Vuomerkityn IPv4-liikenteen lähetys

Vuomerkityn IPv4-liikenteen lähetykseen ATM-ympäristössä (Transmission of Flow Labelled IPv4 on ATM Data Links) varten on muodostettu standardi /22/, jota noudatetaan Ipsilon-ympäristössä. Standardi määrittää IP-kehysten kenttien muokkauksen ja poistot Ipsilon-järjestelmän sisällä ja IP-kehysten lähetysmuodon sellaisiin järjestelmiin, jotka eivät tue Ipsilon-protokollia.

Standardi määrittelee vuotunnuksen, jonka sisältönä on ATM-yhteyden VPI/VCI-tunniste. Vuotunnusta käytetään IFMP-ohjausprotokollan viesteissä. Tunnus muodostuu ATM UNI-solun ensimmäisestä 32 bitistä, joista 4 ensimmäistä (=GFC-kenttä) ei huomioida. Vuotunnuksen rakenne on esitetty kuvassa 5-5 (vrt. kuva 1-1). Yksi rivi kuvassa 5-5 vastaa 28 bittiä eli ATM/UNI-solun kolmea ensimmäistä kenttää.



Kuva 5-5: Vuotunnuksen rakenne /22/

Lisäksi standardi määrittelee IPv4-pakettien kehystystavan ATM-siirtotien yli silloin, kun käytössä on IFMP-vuonohjausprotokolla ja silloin kun käytetään RFC 1483:n määrittelemää LLC/SNAP-kehystystapaa (kts. myös luku 3). ATM-spesifisiä funktioita, kuten verkonhallintasoluja, solun hukkaamisprioriteetin tarkistusta ja ABR-liikenteen ohjaussoluja, ei Ipsilon-järjestelmissä toteuteta. Ipsilon-ympäristössä on varattuja virtuaaliyhteyksiä kaksi kappaletta: Yksi tyhjille soluille (VPI = 0 ja VCI = 0) ja toinen (VPI = 0 ja VCI = 15) oletus-tyyppistä pakettien kehystystapaa (taulukko 5-2) käyttävälle liikenteelle. Kaikki IFMP-viestit lähetetään oletus-tyyppisesti kehystettynä.

Taulukko 5-3: Tietovuotyypit vuomerkityn IP-liikenteen lähetyksessä /22/

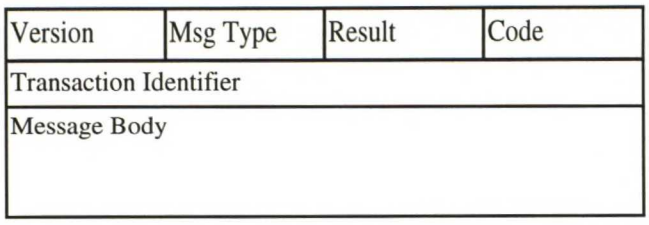
Tietovuotyyppi	Sisältö	Sovitus	MTU	Ohjaus
Oletus	TCP/IP	LLC/SNAP + AAL-5 CPCS-PDU	Vapaa	Oletusmuoto
Tyyppi 0	TCP/IP	AAL-5 CPCS-PDU	1500 tavua	IFMP Flow Type 0-redirect viesti
Tyyppi 1	muokattu TCP/IP	AAL-5 CPCS-PDU	1484 tavua	IFMP Flow Type 1-redirect viesti
Tyyppi 2	muokattu TCP/IP	AAL-5 CPCS-PDU	1492 tavua	IFMP Flow Type 2-redirect viesti

Vuotyypit 1 ja 2 lähetetään, siten että niiden otsikkotietoja on muokattu. Kummastakin vuotyypistä on poistettu TCP/IP-kehyksen version-, IHL-, TTL-, Source Address-, Destination Address-, Source Port- ja Destination Port-kentät. Lisäksi vuotyyppi 1 tapauksessa otsikosta on poistettu myös TOS- ja Protocol-kentät. Vuotyyppien 1 ja 2 vuotunniste muodostuu TCP/IP-kehyksen poistetuista tiedoista ja jokainen verkkoelementti, joka pyytää vuon uudelleenohjausta varastoi vuotunnisteen IP-kehyksen uudelleenmuodostamiseksi yhteyden päätepisteessä tai Ipsilon-ympäristön rajapinnalla. Lisäksi vuotunniste lähetetään IFMP ohjausprotokollan viestin Message Body -osassa pyydettäessä vuon uudelleenohjausta. Vuotyypin valinta perustuu siihen, miten vuon kytkemispäätökseen on päästy. Mikäli kytkemispäätös perustuu havaittuun liikenteen pitkäikäisyyteen, käytetään vuotyyppiä 1. Mikäli kytkemispäätös on tehty suoraan TCP/IP-kehyksestä havaittujen osoite/portti-kombinaatioiden avulla, käytetään vuotyyppiä 2. /22/

5.3 Yleinen välityslaitteiston hallintaprotokolla - GSMP

Yleinen välityslaitteiston hallintaprotokolla (General Switch Management Protocol, GSMP) on standardi, joka määrittelee erään tavan hallita ATM-välityslaitteistoja (solmuja ja kytkimiä). Protokollan toiminteisiin sisältyy mm. virtuaaliyhteyksien muodostus, purku ja hallinta, kytkimen sisään- ja ulostuloporttien hallinta se-

kä virtuaaliyhteyksien liikennöintiaktiivisuuden tarkkailu. GSMP-protokolla korvaa Ipsilon-ympäristössä yhdessä IFMP-protokollan kanssa signalointiprotokollat sekä erilaiset ATM-välityslaitteiston hallintaprotokollat. GSMP-protokolla on ominaisuuksiltaan toistaiseksi hyvin yksinkertainen ja sen kehitystyö jatkuu edelleen. GSMP-viestit lähetetään oletus-muotoisesti (taulukko 5-2) pakattuna. GSMP-protokollan viestin yleinen rakenne on esitetty kuvassa 5-6. Yksi rivi kuvassa vastaa 32 bittiä.



Kuva 5-6: GSMP-viestin yleinen rakenne /24/

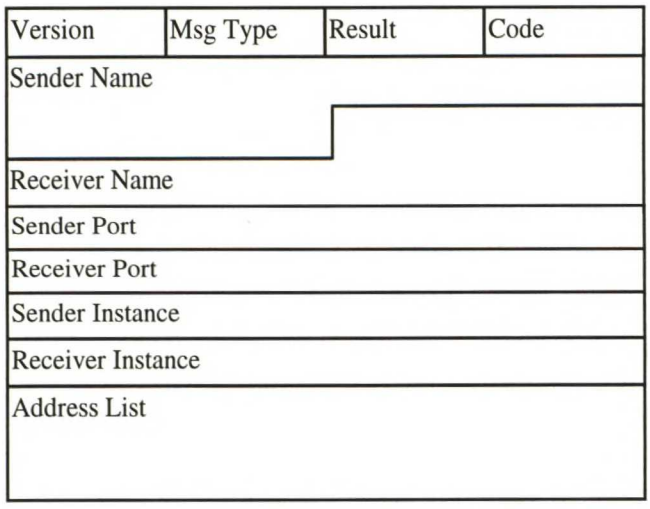
Luettelo GSMP-protokollan sisältämistä toiminteista ja niiden toteuttamisessa tarvittavista sanomatyypeistä on esitetty taulukossa 5-4.

Taulukko 5-4: GSMP-protokollan toiminnot ja viestityypit /24/

Toiminto	Viestityypit
Yhteyksien hallinta	Add Branch, Delete Branch, Delete Tree, Verify Tree, Delete All, Move Branch
Porttien hallinta	Port Management
Tilastotietojen hallinta	VC Activity, VC Statistics, Port Statistics
Asetustietojen hallinta	Switch Configuration, Port Configuration, All Ports Configuration
Tapahtumien hallinta	Port Up, Port Down, Invalid VC/VP, New Port, Dead Port

Toiminteen vaatimat tiedot lähetetään GSMP-viestin Message Body-osassa (kts. kuva 5-4).

Lisäksi GSMP-protokollassa on määritelty IFMP-naapuriprotokollaa toiminnallisesti vastaava GSMP-naapuriprotokolla (GSMP Adjacency Protocol), jonka tehtävänä on muodostaa yhteydet verkossa sijaitseviin viereisiin välityslaitteistoihin, ylläpitää tietoja ja havainnoida muutoksia naapurielementeistä havaituissa tilatiedoissa. GSMP-naapuriprotokollan viestin rakenne on esitetty kuvassa 5-7. Yksi rivi kuvassa vastaa 32 bittiä.



Kuva 5-7: GSMP-naapuriprotokollan viestin yleinen rakenne /24/

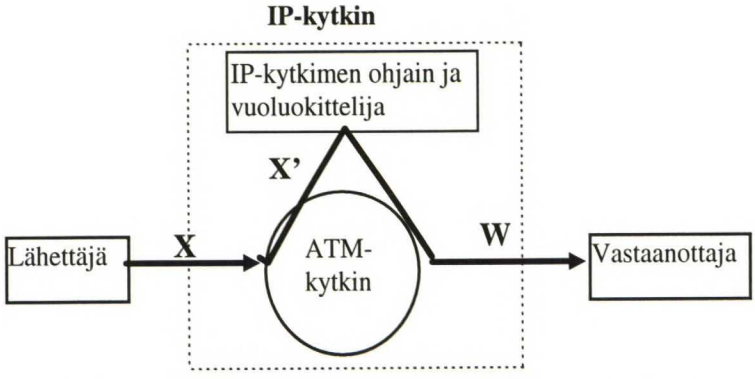
Erityisesti GSMP-naapuriprotokollaviestistä on huomattava, että siinä käytetään yhteyden muodostavien laitteiden 48 bittisiä IEEE 802 MAC-osoitteita mikäli ne vain ovat saatavilla. Code -kentän arvot ja toiminta vastaavat IFMP-naapuriprotokollan OpCode -kentän vastaavia toimintoja. /24/

5.4 IP-kytkennän toiminta

Seuraavassa IP-kytkennän toimintakuvauksessa tarkoitetaan lähettävällä ja vastaanottavalla naapurielementillä, tietyn vertailupisteen suhteen, loogisesti edellistä ja seuraavaa päätelaitetta tai IP-kytkintä.

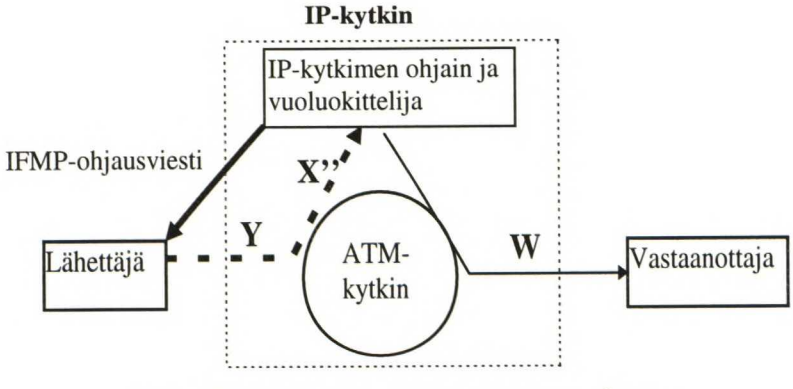
IP-kytkennän toiminta Ipsilon-ympäristössä perustuu yksisuuntaisille virtuaaliyhteyksille, joten yksittäinen portti omistaa VC/VP-numeroavaruuden, joka kuuluu yksinomaan tulevalle yhteydelle. Kun oletusyhteydeltä X (VP=0, VC=15) saapuu IP-paketti, se ohjataan ennalta valitulle vapaalle yhteydelle X' kontrolliprosessoriin. Kontrolliprosessori tekee reitityspäätöksen normaaleihin IP-reititysprotokolliin nojautuen, ja tämän jälkeen IP-paketit lähetetään edelleen alemmille kerroksil-

le sovitettavaksi ATM-järjestelmään. Tällöin järjestelmä toimii kuten mikä tahansa reititin, joka käyttää ATM-verkkoa siirtotienä (kuva 5-8).



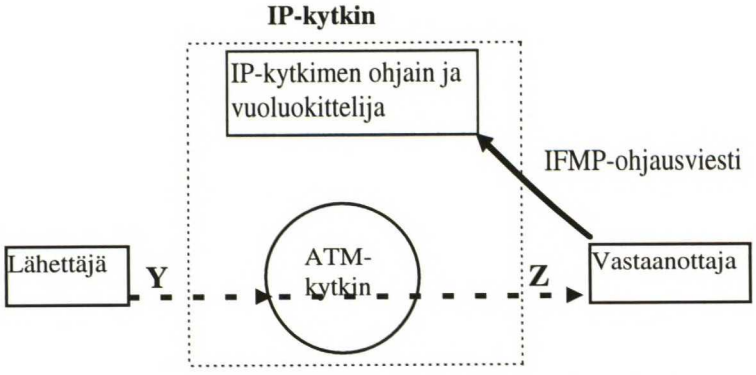
Kuva 5-8: Ipsilon-järjestelmän toiminta reitittimenä

Mikäli liikenteen reitityksen yhteydessä havaitaan sellainen tietovuo, joka täyttää tietyt edeltäkäsin asetetut vaatimukset, voidaan ko. tietovuo kytkeä omalle virtuaaliyhteydelleen. Tällöin IFMP-ohjausprotokollan ohjausviestillä esitetään lähettävälle naapurielementille pyyntö yhteyden X ohjaamisesta omalle virtuaaliyhteydelleen Y. Ennen pyynnön esittämistä on muodostettu yhteys Y:n ja uuden kontrolliyhteyden X'' välille. Ohjauspyyntöä ei kuitata, vaan ensimmäinen paketti uudella yhteydellä ilmaisee ohjauspyynnön hyväksymisen. Tämän jälkeen kaikki solut yhteydellä Y ohjataan suoraan yhteydelle X'' , jossa reititystapahtuma toimii nopeammin, koska reitityspäätös on pidetty muistissa ja päätöstä ei tarvitse tehdä uudestaan. Kyseessä on ns. soft-state reititys. Tämä muodostaa ensimmäisen vaiheen verkon välityskyvyn tehostamisessa perinteisiin reitittimiin verrattuna. Tilanne on esitetty kuvassa 5-9.



Kuva 5-9: Soft-state reititys ja vuonohjaus

Kun vastaanottava naapurielementti pyytää ohjaamaan yhteyden W uudelle yhteydelle Z, ja kun yhteys on muodostunut, IP-kytkimeen saapuvia IP-paketteja ei tarvitse ohjata kontrolliprosessorille reititettäväksi, vaan ne voidaan ohjata suoraan ATM-välityslaitteiston kytkentäkentän läpi. Tällä menetelmällä Ipsilon-ympäristössä saavutetut tiedonsiirtonopeudet verrattuna perinteisiin reititysympäristöihin ovat merkittävästi suurempia. Suora IP-kytkentä Ipsilon-ympäristössä on esitetty kuvassa 5-10.



Kuva 5-10: IP-kytkentä Ipsilon-järjestelmässä

Mikäli IP-kytkin hyväksyy IFMP-ohjausviestin, se samalla muuttaa IP-kehysten esitystapaa jonkin vuotyypin mukaiseksi. Lisäksi IP-kytkin suorittaa aikavalvontaa kaikilla ohjatuilla yhteyksillä, ja mikäli näillä ei esiinny liikennettä yhteys puretaan ja palataan takaisin tilaan, jossa saapuneet IP-kehykset ohjataan kontrolliprosessorille reitityspäätöksen tekemistä varten. Mikäli yhteydellä esiintyy liikennettä, tehdään yhteyden uudistuspyyntö lähettävälle naapurielementille. Kaikenkaikkiaan vuonohjaus on täysin itsenäistä ja paikallista toimintaa. Yhdenkään verkon elementin ei ole pakko muodostaa erillisiä yhteyksiä IP-tietovoille, eikä yksikään verkkoelementti voi yksinään ohjata tietovuota uudelle yhteydelle. Mikäli jokin IP-kytkin ei halua ohjata IP-tietovoita omille yhteyksilleen, tai sen pyrkimyksiä ohjaamiseen ei tueta muualla verkossa, se toimii kuten tavallinen reititin. /19, 20/

5.4.1 Monilähetysliikenne Ipsilon-ympäristössä

Ipsilon-järjestelmän mukainen IP-kytkin tukee monilähetysliikennettä automaattisesti. Reititysprotokollan selvitettyä minne monilähetysviesti ohjataan, voidaan multicast-vuot ohjata omille virtuaaliyhteyksilleen. Mikäli nämä monilähetysyhteydet on jo kytketty omille virtuaaliyhteyksilleen, voidaan myös hyödyntää ATM-

kytkinkentän mahdollista multicast-palvelua, so. ATM-solujen monistusta. Monilähetysyhteyksillä kulkeva tieto voidaan lähettää myös kontrolliprosessorille, jolloin nekin verkon jäsenet, jotka eivät ole ohjanneet monilähetysyhteyksiä omille virtuaaliyhteyksilleen, voivat vastaanottaa monilähetyssanomia. /19/

5.5 Yhteenveto

IP-kytkentä on uudenlainen ajattelutapa toteuttaa internet-verkkoja. Perinteisten reitittimien kapasiteettirajoitusten muodostaessa pullonkauloja internet-verkoissa IP-kytkimet tarjoavat suorituskyvyn parannusta. Kriittinen tekijä IP-kytkentää muodostettaessa on yhteyden liikenneprofiilin määrittäminen. Yhteys kannattaa kytkeä, mikäli lähetettävää tietoa on kohtuullisen paljon tai IP-vuon kestoaika on melko pitkä. Lisäksi täytyy vaatia, että yhteydellä lähetetään kohtuullisen usein, jotta ei turhaan varattaisi kaistanleveyttä verkosta. Ipsilon-järjestelmässä kytkettävä IP-vuo on ymmärretty yksisuuntaiseksi, joten on mahdollista, että eräistä palvelumuodoista, esimerkiksi pääteyhteyksistä, kytkettäisiin vain toiseen suuntaan muodostettu yhteys.

Tietovuon kytkemisinformaation kerääminen sekä ao. informaation lähettäminen yhteyden edelliselle osapuolelle vaatii hetken aikaa ja tuottaa hieman lisää liikennettä (noin 10 IP-pakettia) verkkoon. Tämän huomioonottaminen vaatii joko hyvin ajoitettua vuonohjausta tai suuria puskureita. Käytännössä suuret puskurit lienevät paras toteutettavissa oleva tapa, joilla tietovuohon kuuluvia soluja voidaan varastoida, kunnes yhteydet kumpaankin suuntaan on luotu. Erityisesti TCP-protokollaa käyttävien yhteydellisten palveluiden luonteeseen kuuluu, että yhteys muodostetaan ennen kuin tiedon lähetys alkaa. Joten jos tietovuo voidaan tunnistaa jo ensimmäisistä paketeista, voidaan olettaa, että kun tiedonsiirto yhteydellä varsinaisesti alkaa, on tietovuo jo ehditty kytkeä suoraan ATM-kytkentäkentän läpi.

Ipsilon-protokollia hyödyntävät ATM-välityslaitteistot, Ipsilon-kytkimet, käyttävät standardoituja ja koeteltuja internet-reititysprotokollia, joten reitityksen onnistuminen IP-kytkimissä on vankalla pohjalla. Lisäksi varsinainen yhteystaulukoiden muodostus tapahtuu GSMP-protokollan avulla seuraavalta verkon elementiltä tulleiden viestien perusteella, joten raskaat signalointiprotokollat eivät kuormita verkkoa.

Ipsilon-järjestelmän suorituskyky, perinteisiin verkkoympäristöihin verrattuna, paranee kahdessa vaiheessa: Ensimmäinen parannus tulee reititystietojen muistamisesta, joskin tämän tuoma parannus on marginaalinen. Toinen parannus - tällä kertaa selkeämpi - saavutetaan, kun verkossa on vähintään kolme peräkkäistä Ipsilon-protokollaa hyödyntävää elementtiä, jolloin IP-tietovuot voidaan reitittää keskimmäisessä Ipsilon-elementissä omille virtuaaliyhteyksilleen.

Ipsilon-järjestelmä tukee myös palvelun laadun (QoS) määrittämistä yhteydelle. Tämä on mahdollista, koska reitityspäätöksiä ja yhteyksiä muodostettaessa on tarkasti tiedossa käytettävä internet-palvelu eli TCP-porttinumero. Palvelun laatua määritettäessä voidaan ottaa huomioon TCP/IP-kehyksestä saatavat tiedot tai muiden protokollien avulla välitetyt pyynnöt tietyistä palveluluokista.

6 Liikennemittaukset

6.1 Yleistä

Tässä luvussa käsitellään erikokoisten TCP/IP-liikennettä välittävien tietoliikenneverkkojen liikennemittauksista saatuja tuloksia. Mallina tämän työn puitteissa tehdyille mittauksille toimii suurehkon Amerikan Yhdysvaltain itärannikolla sijaitsevan runkoverkon liikenteestä tehty tutkimus, joka käsitellään tässä työssä ensimmäisenä. Tämä tutkimus määrittää muun muassa sen, millaisia tietoja pienemmistä verkoista pyritään analysoimaan; Tuloksina on tarkoitus saada mittausten välillä keskenään vertailukelpoista aineistoa, jotta näistä voitaisiin vetää kohtuullisen päteviä johtopäätöksiä erilaisten ATM-tekniikoiden ja erityisesti IP-kytkennän soveltuvuudesta eri kokoluokan verkkoihin. Edelleen mittausten tarkoituksena on saada perustaa pohdinnoille, mikä edellä esitetyistä ATM-tekniikan sovellutuksista sopii mahdollisimman hyvin internet-liikenteen välitykseen eri kokoluokkien verkoissa. Erityisesti keskitytään selvittämään IP-kytkennän soveltuvuutta internet-liikenteen välityksessä.

Kahden pienemmän verkon mittaus tehtiin *TCPDUMP*-nimisellä tietokoneohjelmalla, jolla voidaan rekisteröidä verkossa kulkevaa liikennettä halutulla tarkkuudella. Ohjelman tulosteena (kts. Liite 1) saadaan tässä työssä vaadittavat tiedot: IP-paketin aikaleima, lähde- ja kohdeosoite, TCP-paketin lähde- ja kohdeportit sekä paketin sisältämän tiedon määrä tavuina. Ohjelma on valittu tähän työhön myös siksi, että se ei vahingossakaan mahdollista verkossa liikkuvan tiedon yksityiskohtaista seuraamista. Mittaustiedostoista selviävät ainoastaan lähde- ja kohdekoneiden osoitteet ja käytetty TCP-palveluportti.

6.2 Todellisen liikenteen mittaukset ja analyysi

6.2.1 Liikenneanalyysi

Jatkossa esiteltävien liikennemittausten analysointi perustuu seuraavan kaltaiseen nelivaiheiseen menettelyyn /20, 21/.

1: Tehdään liikennemittaus IP-protokollan mukaisia paketteja kuljettavasta verkosta. Mittaus tehdään IP-pakettitasolla ja jokaisesta paketista talletetaan sen aikaleima, paketin sisältämät IP-osoitteet (lähettäjä ja vastaanottaja), paketin sisältä-

mät tiedot välitettävästä ylemmän tason protokollasta (IP-paketin protocol-kenttä tai TCP-paketin porttinumerot) ja välitetyn paketin sisältämän tiedon pituus tavuina.

2: Tehdään yksinkertaistettu vuoanalyysi, jossa jokainen uusi IP-osoitepari aiheuttaa uuden vuon muodostamisen. Seuraavista paketeista merkitään kuuluvaksi samaan vuohon ne paketit, joilla on sama IP-osoitepari kuin ensimmäisellä tähän vuohon kuuluneella IP-paketilla. Jos edellisen paketin lähetyksestä asianomaisella vuolla on kulunut yli 60 sekuntia tuhotaan vanha vuo ja luodaan uusi vuo, kun seuraava paketti saapuu (taulukko 6-1). Vuon kokonaiskesto lasketaan ensimmäisen ja viimeisen vuohon kuuluvan paketin lähtöajoista.

Taulukko 6-1: Vuonmuodostuksen perusehdot

	Vuonmuodostus
Paketit	-
Aika	< 60 s (kahden paketin välinen aika)
IP-osoitepari	x

Tämän perusteella voidaan määritellä, mikä on muodostettujen voiden lukumäärä ja voilla lähetettyjen pakettien suhde vuon kestoon eli elinaikaan. Tämä tiedon avulla voidaan tehdä päätelmiä, missä määrin verkossa esiintyvä liikenne yleisesti ottaen soveltuu IP-kytkentään.

3: Tehdään edellisen kohdan kaltainen vuoanalyysi erikseen kaikille niille TCP-tason protokollille, joita voissa esiintyy vähintään tietyn suhteellisen osuuden verran (tässä tutkimuksessa 0,05 %). Näiden tietojen avulla lasketaan kunkin protokollan osuus kaikista voista, paketeista ja tiedon määrästä. Lisäksi määritetään keskimääräiset arvot sille, kuinka monta vuota sekunnissa syntyy ja montako pakettia sekunnissa vuolla lähetetään. Edelleen määritetään keskiarvoiset suureet vuon kestolle sekä pakettien määrälle vuota kohti.

Tämän kohdan perusteella pyritään selvittämään, mitkä palvelut (TCP-portit) ovat sellaisia, että niille voitaisiin perustaa oma virtuaaliyhteys. Yleisesti etsitään sellaisia liikennevirtoja, joissa lukumääräisesti mahdollisimman vähillä voilla lähetetään mahdollisimman paljon liikennettä eli paketteja tai dataa. Tällaisessa tilanteessa yhteydenmuodostuksen osuus liikenteen välittämisessä ei kuormita suhteet-

tomasti itse ATM-kytkinlaitteistoja eikä yhteydenmuodostuksen aiheuttama liikenne rasita verkkoa liiaksi.

4: Viimeiseksi tarkastellaan IP-kytkentää ikäänkuin käänteisesti ja pyritään määrittämään kytkentäkynnys. Kytkentäkynnys vastaa sitä reitittimen vastaanottamaa pakettimäärää, jonka jälkeen vastaanotettu IP-tietovuo voidaan kytkeä omalle virtuaaliyhteydelleen Ipsilon-protokollien mukaisesti. Mittausten perusteella voidaan määrittää vaatimukset vuon muodostamisen nopeusvaatimuksille, ja määrittää reitittimelle siirtyvien pakettien lukumäärä. Reitittimelle on laskettu sen kuormitus eri kytkentäkynnyksillä, kun vuonmuodostus vaatii joko 10 tai 25 paketin lähettämisen.

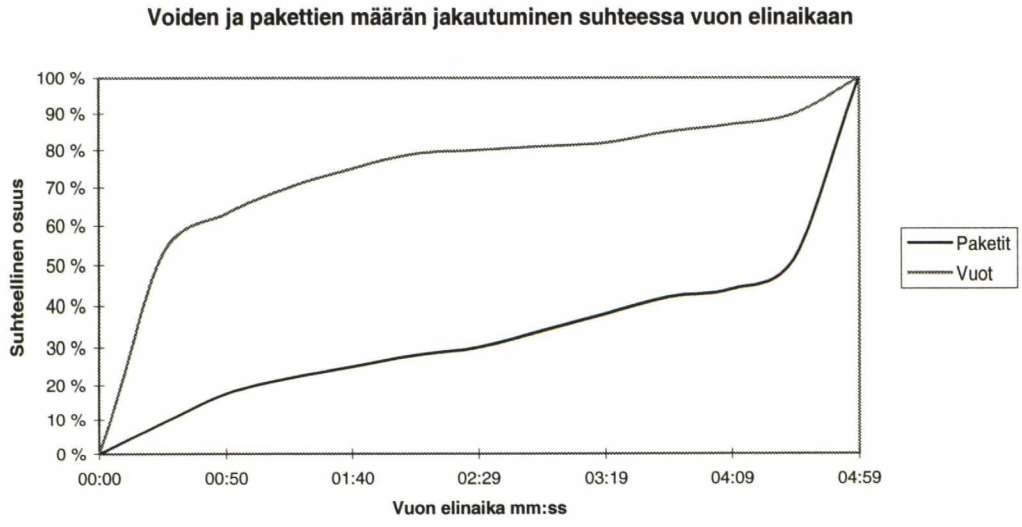
Lisäksi määritellään kokonaiskuormitusfunktio reitittimelle ja vuonmuodostajalle:

$$\textit{Kokonaiskuormitus} = \textit{reititetyt paketit} + \textit{yhteyden muodostuksen vaatimat paketit} \quad (1)$$

Tätä (1) pyritään minimoimaan optimoimalla kytkentäkynnystä. Tällä menettelyllä on se etu, että kytkentäkynnyksen arvoa voidaan muuttaa verkossa esiintyvän liikenteen mukaan ja estää näin IP-kytkimen resurssien hallitsematonta käyttöä. Kokonaiskuormitusfunktion arvot on tässä tutkimuksessa määritelty silloin, kun yhteydenmuodostus vaatii 10 tai 25 paketin lähettämisen.

6.2.2 Suuren runkoverkon liikenteen analyysi (Ipsilon)

Ipsilon-protokollien vuonohjaus perustuu internet-runkoverkossa tehtyyn liikennemittaukseen ja sen analysointiin. Liikennemittaus on tehty Yhdysvaltain itärannikolla sijaitsevasta FDDI-renkaasta, joka on yhteydessä itärannikon alueen internet-runkoverkkoon. Mittaus on tehty myöhään iltapäivällä ja sen kesto oli viisi minuuttia. Mittaustuloksina on kertynyt likimain 5 miljoonaa pakettia. Tutkittaessa yksinkertaisella vuoanalyysillä liikennettä havaittiin, että 64 % voista on alle minuutin mittaisia, ja että näillä voilla lähetetään 16 % kaikista paketeista. Tarkasteltaessa sitä 10 % yhteyksistä, jotka muodostavat liikenteen pitkäkestoisimmat yhteydet, huomataan että näillä siirtyy hieman yli 50 % kaikista paketeista. Kuvassa 6-1 on esitetty likimääräinen kuva siitä, miltä edellä kuvattu tilanne näyttää graafisessa tarkastelussa.



Kuva 6-1: Kumulatiivinen voiden ja pakettien jakauma suuressa runkoverkossa vuon elinaikaan verrattuna /20/

Kuvan 6-1 perusteella on tehty päätelmä, että pitkäkestoiset ja paljon tiedon siirtoa sisältävät yhteydet voidaan kytkeä omille virtuaaliyhteyksilleen.

Suuren runkoverkon liikennemittauksen analyysi protokollittain on esitetty taulukossa 6-2. Analyysi on tehty kohdan 6.2.1 mukaan.

Taulukko 6-2: Runkoverkon liikenneanalyysi /20/

Protokolla	Portti	Kytkentä	%vuo	%paketti	%tavu	vuo/s	paketti/s	Keskim.kesto	Paketti/vuo
IP		*	0,04	2,79	2,57	0,09	456	173,1	2307
TCP/ftp-data	*20*	*	0,76	12,09	15,18	2,17	2018	118,2	525
TCP/ftp-cntrl	*21*		1,55	0,74	0,23	6,5	124	38,6	16
TCP/telnet	*23*	*	1,39	4,81	1,61	4,24	803	114,3	114
TCP/smtp	*25*		10,26	4,8	2,82	49,49	802	18,2	15
UDP/dns	*53*		45,3	5,57	3,04	216,56	929	15,4	4
TCP/gopher	*70*	*	0,45	0,54	0,55	1,87	91	43,3	40
TCP/http	*80*	*	17,94	40,21	41,53	72,98	6717	56,5	74
TCP/pop-v3	*110*		0,08	0,05	0,03	0,41	9	27	21
TCP/authent	*113*		2,12	0,19	0,05	10,54	32	9	3
TCP/nntp	*119*	*	0,35	6,56	6,59	0,68	1096	176,7	627
UDP/ntp	*123*		5,01	0,2	0,06	25,02	33	1,37	1,3
TCP/netbios	*139*	*	0,03	0,08	0,15	0,11	14	69,8	82
UDP/snmp	*161*		1,35	0,26	0,11	6,14	43	17,9	6
TCP/login	*513*	*	0,09	0,24	0,14	0,31	41	88,1	92
TCP/cmd	*514*	*	0,01	0,13	0,07	0,06	21	49,1	316
TCP/audio	*1397*	*	0	2,2	2,62	0,01	367	167,9	15653
TCP/AOL	*5190*	*	0,18	0,46	0,38	0,51	77	129,8	84
TCP/X-11	*600x*	*	0,08	0,66	0,53	0,18	111	160,6	276

Mittauksesta on analysoitu eri TCP-porttinumeroiden perusteella muodostettujen yhteyksien esiintymistä. Http-protokollan tuloksista tulee huomata, että todellisissa verkkoympäristöissä jokainen http-protokollan avulla siirrettävä elementti lähe-

tetään uudella yhteydellä, jossa IP-osoitteet pysyvät samoina, mutta jossa elementin vastaanottajan porttinumero vaihtuu koko ajan. Käytännössä tämä tarkoittaa sitä, että http-protokollan siirrossa tapahtuu huomattavasti useammin vuonmuodostusta ja yhteydet ovat keskimäärin lyhyempiä, kuin mitä ylläoleva taulukko antaa ymmärtää. Tässä analyysissä on kuitenkin otettu huomioon vain IP-osoitteiden väliset http-yhteydet. Jatkossa esiteltävissä mittauksissa on yhteneväisyyden vuoksi tehty samoin.

Taulukon 6-1 mukaan tarkastelussa on mukana 82 % kaikista lähetetyistä paketeista. Yhteyden kytkemiskelpoisuudelle on annettu seuraava perusehto: Jotta yhteys voitaisiin kytkeä, täytyy sen keskimääräisen keston olla vähintään 20 sekuntia ja yhteydellä siirrettyjen pakettien lukumäärän täytyy ylittää 40 kpl (taulukko 6-3) /20/. Yhteydellä siirretyn tiedon määrään ei oteta kantaa vuon kytkentäehdoissa.

Taulukko 6-3: Vuon kytkentäehdot

	Kytkentäehdot
Paketit	40 pkt (keskimääräinen arvo)
Aika	20 s (keskimääräinen arvo)
IP-osoitepari	x

Kun ylläolevia ehtoja sovelletaan, on havaittu, että noin 71 % kaikesta runkoverkon liikenteestä voitaisiin tarvittaessa kytkeä suoraan omille erillisille virtuaaliyhteyksilleen. Nämä vuot muodostavat noin 21 % kaikista voista, joten yhteydenmuodostuksen aiheuttama kuorma on todettu kohtuulliseksi suhteessa saavutettuun hyötyyn. Vaadituksi vuonmuodostusnopeudeksi on tämän analyysin perusteella määritelty noin 92 vuota sekunnissa.

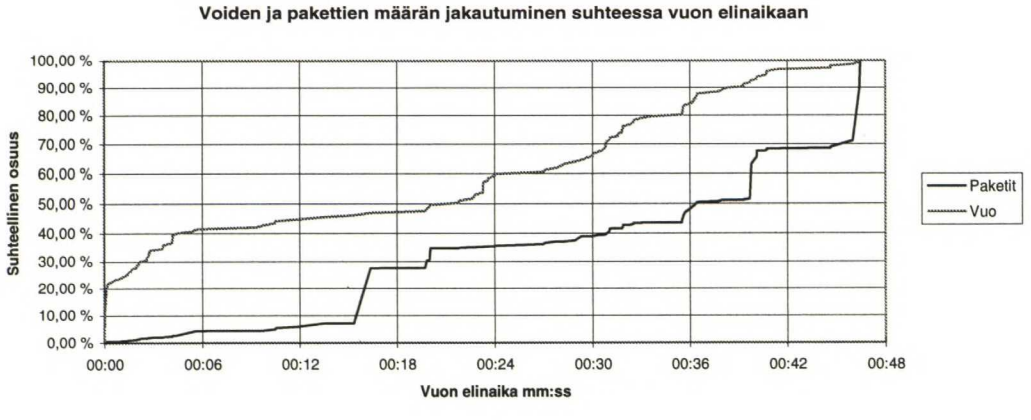
Tämän jälkeen on tarkasteltu kytkemispäätöksen tekemistä yhdellä vuolla vastaanotettujen pakettien määrän perusteella. Tätä suuretta kutsutaan kytkentäkynnykseksi, joka ilmaisee saapuneiden pakettien määrän vuolla ennen vuon kytkemistä omalle virtuaaliyhteydelleen. Etsittäessä kytkentäkynnystä, jolla vaadittava yhteydenmuodostusnopeus olisi sama kuin protokolla-analyysin avulla saatu, havaitaan, että kun yhteydellä on lähetetty 13 pakettia, on vuonmuodostusnopeus sama kuin protokolla-analyysin perusteella saatu yhteydenmuodostusnopeus.

Optimoitaessa reitityskomponentin kuormitusta 10 paketin ja 25 paketin vuonmuodostuksella löydetään kuormitusfunktiolle (1) minimi vastaavasti kytkentäkynnyksen arvoilla 5 pakettia ja 15 pakettia /20/. Verrattaessa täysin reitittävään ympäristöön saavutetaan vastaavasti yli 80 % ja 70 % vähennys reitityskomponentin tekemässä työssä. /20/

6.2.3 Runkoverkon liikenteen analyysi: Case Sähköosaston runkoverkko

Suoritettaessa liikenneanalyysiä Helsingin Teknillisen Korkeakoulun Sähkö- ja tietoliikenneosaston runkoverkossa vajaan minuutin ajan eräänä lokakuisena työpäivänä vuonna 1996 noin klo 10 saatiin pakettien määräksi 16365. Runkoverkko on 10 Mbit/s Ethernet-verkko, joka on yhteydessä koko Otaniemen aluetta yhdistävään FDDI-renkaaseen. Mittaustulosten analyysi perustuu samoille periaatteille, kuin edellä esitetty suuren runkoverkon analyysi. Mittausajanjakso on lyhyt, koska analyysiin käytetty ohjelmisto ei pysty käsittelemään suuria määriä rivejä mittaustiedostosta. Tulokset ovat kuitenkin suuntaa antavia ja näin ollen niitä voidaan varovaisuutta noudattaen käyttää päättelyssä hyväksi.

Aluksi tutkittiin ainoastaan IP-osoitepareja ja tehtiin tästä yksinkertainen vuoanalyysi, jonka tulos on esitetty kuvassa 6-2.



Kuva 6-2: Kumulatiivinen voiden ja pakettien jakauma pienessä runkoverkossa vuon elinaikaan verrattuna

Kuvasta 6-2 nähdään, että likimain 50 % edellä mainituin perustein muodostetuista voista on alle 20 sekunnin mittaisia ja näissä siirtyy noin 30 % kaikista paketeista. Jos tarkastellaan sitä 10 % osuutta, joka muodostaa kaikkien pitkäkestoisimmat vuot, huomataan että näillä voilla siirtyy likimain 50 % kaikista paketeista.

Tulos vastaa tässä vaiheessa jotakuinkin edellisen kohdan mittauksista tehdyn perusanalyysin tuloksia.

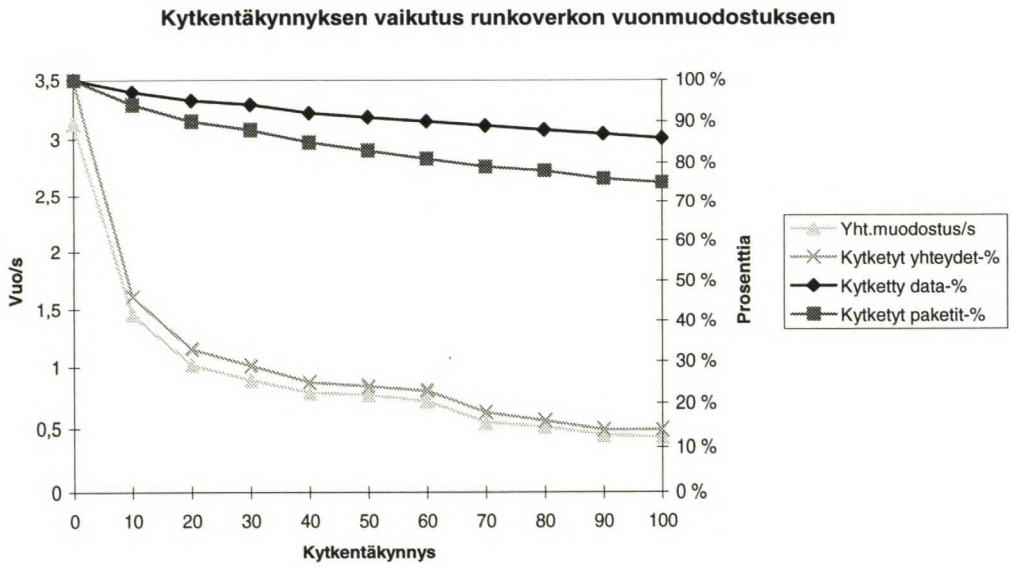
Protokolla-analyysiä varten mukaan otetaan ne protokollat, joiden muodostamien yhteyksien siirretty pakettimäärä on vähintään 0,05 % kaikista lähetetyistä paketeista. Protokolla-analyysiin saatiin näin mukaan 99,34 % kaikista lähetetyistä paketeista. Analyysin tulokset on esitetty taulukossa 6-4.

Taulukko 6-4: Pienen runkoverkon liikenteen protokolla-analyysi

Protokolla	Portti	Kytkentä	%vuo	%paketti	%tavu	vuo/s	paketti/s	Keskim.kesto	Paketti/vuo
TCP/ssh	22	*	2,63 %	4,64 %	0,77 %	0,031	3,97	31,9	127
TCP/http	80		14,04 %	32,76 %	54,45 %	0,103	17,31	9,7	168
dos			0,88 %	0,34 %	0,31 %	0,057	1,58	17,7	28
TCP/telnet	23	*	7,89 %	6,32 %	0,85 %	0,036	2,07	27,8	58
UDP/dns	53		19,74 %	11,30 %	3,50 %	0,086	3,53	11,6	41
UDP/pop-3	110		4,39 %	0,59 %	0,04 %	0,463	4,44	2,2	10
TCP/www-proxy	8000		0,88 %	0,15 %	0,25 %	0,277	3,46	3,6	13
TCP/Xwin	60xx	*	5,26 %	33,75 %	7,69 %	0,044	20,38	22,6	460
TCP/login	513		1,75 %	0,26 %	0,20 %	0,108	1,16	9,3	11
UDP/finger	79		0,88 %	0,07 %	0,01 %	13,333	80,00	0,1	6
UDP/ntp	123		2,19 %	0,06 %	0,01 %	0,109	0,22	9,1	2
nfs			4,39 %	0,26 %	0,13 %	0,081	0,34	12,4	4
UDP/sunrpc	111		16,23 %	0,82 %	0,16 %	0,131	0,48	7,6	4
TCP/netbios-ssn	139	*	2,63 %	7,44 %	30,13 %	0,032	6,57	30,9	203
nterm			0,88 %	0,56 %	1,16 %	0,178	8,17	5,6	46

Yhteyden kytkemisehdot on esitetty taulukossa 6-3. Kun näitä ehtoja sovelletaan, on havaittu, että noin 52 % kaikesta liikenteestä voidaan kytkeä omille virtuaaliyhteyksilleen. Nämä vuot muodostavat 18 % kaikista voista, joten yhteydenmuodostuksen aiheuttama kuorma on kohtuullinen. Vuonmuodostuksen nopeusvaatimukseksi saadaan edellä olevan perusteella noin 0,9 vuota sekunnissa. Mikäli vuo muodostettaisiin kaikille havaituille voille, olisi vuonmuodostusnopeus noin 4,1 vuota sekunnissa. Protokolla-analyysin tuoma kuormanpienennys vuonmuodostuksessa on siis noin 78 %. Jos kytkettäviin voihin otetaan mukaan kaksi seuraavaksi kytkentään soveltuvinta protokollaa (http, nterm) saadaan vuonmuodostusnopeudeksi noin 1,6 vuota sekunnissa ja kuormanpienennys vuonmuodostuksessa on noin 60 %.

Tarkasteltaessa vuon kytkemisehtoa siten, että tarkkaillaan vuolla lähetettyjen pakettien määrää ja kytketään vuo omalle virtuaaliyhteydelleen vasta tietyn saapuneen pakettimäärän jälkeen, voidaan tarkastella kytkentäkynnyksen vaikutusta vuonmuodostukseen ja kytketyillä yhteyksillä välitettyjen pakettien ja tiedon määrään. Tämä tarkastelu on tehty kuvassa 6-3.

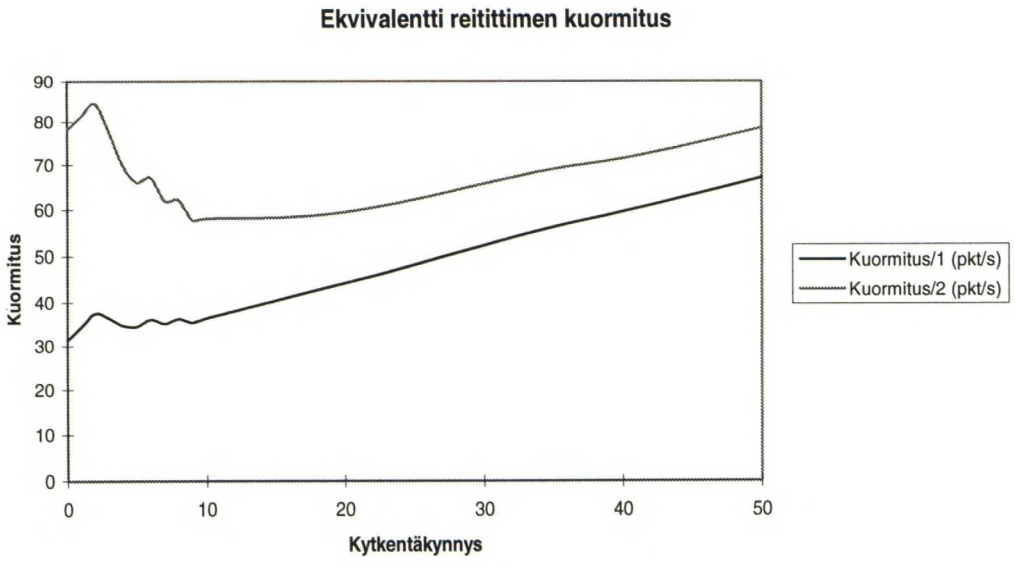


Kuva 6-3: Kytkentäkynnyksen vaikutus vuon muodostukseen runkoverkossa

Etsittäessä kytkentäkynnyksen arvoa, jolla päästäisiin samaan vuonmuodostusnopeuteen kuin protokolla-analyysin perusteella saadaan kuvan perusteella kytkentäkynnyksen arvoksi noin 20 pakettia.

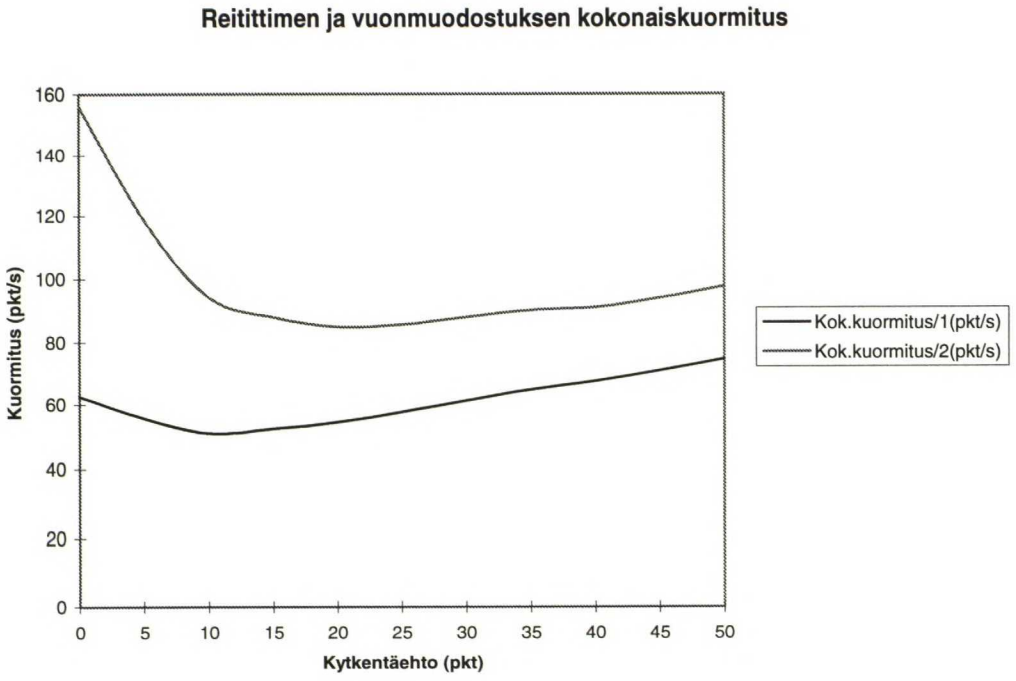
Erityisesti on huomattava, että mikäli vuoluokittelu perustuu puhtaasti protokolla-analyysiin, vuonmuodostuksessa aiheutuva teoreettinen maksimikuorma on noin 30 % suurempi, kuin jos vuonmuodostus tehdään pelkästään vastaanotettujen pakettien määrän perusteella. Tämä johtuu protokolla-analyysin sokeudesta tavallisesti pitkiä yhteyksiä sisältävissä protokollissa esiintyville lyhytaikaisille, ja siten vain muutamia paketteja sisältäville, yhteyksille.

Reitityskomponentin kuormitus kytkentäkynnyksen funktiona 10 paketin ja 25 paketin vuonmuodostuksella on esitetty kuvassa 6-4.



Kuva 6-4: Reititysfunktion kuormitus 10 paketin (kuormitus/1) ja 25 paketin (kuormitus/2) vuonmuodostuksella

Kuvasta 6-4 havaitaan, että kuormitusfunktiolla on minimi 10 paketin ja 25 paketin yhteydenmuodostuksella vastaavasti 5 paketin ja 10 paketin kytkentäkynnyksen kohdalla. Verrattaessa täysin reitittävään ympäristöön saavutetaan vastaavasti 90 % ja yli 80 % väheneminen reitityskomponentin työssä. Viimeiseksi tarkastellaan reitityskomponenttia ja vuonmuodostuskomponenttia yhtenä kokonaisuutena, jonka kokonaiskuormitusta pyritään minimoimaan. Tällainen tarkastelu on esitetty kuvassa 6-5.

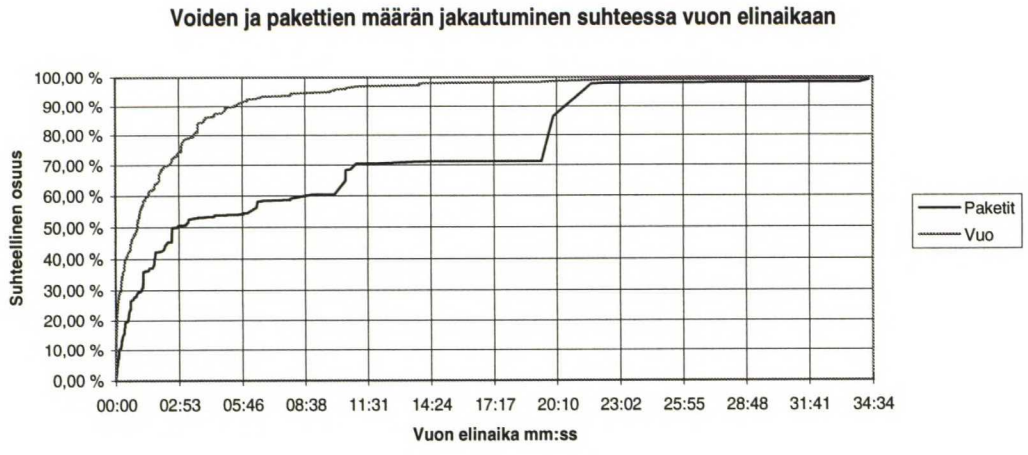


Kuva 6-5: Kokonaiskuormitus reitittimessä ja vuonmuodostajassa 10 paketin (kuormitus/1) ja 25 paketin (kuormitus 2) vuonmuodostuksella

Kuvasta havaitaan, että reititys- ja vuonmuodostuskomponenttien toiminta on optimaalista, kun on vastaanotettu 12 tai 22 pakettia riippuen siitä, vaatiiko vuonmuodostus 10 tai 25 pakettia.

6.2.4 Lähiverkon liikenteen analyysi: Case Teletekniikan laboratorio

Suoritettaessa liikenneanalyysiä Helsingin Teknillisen Korkeakoulun Teletekniikan laboratorion paikallisverkossa noin 35 minuutin ajan eräänä syyskuisena työpäivänä vuonna 1996 noin klo 9.55 - 10.30. saatiin pakettien määräksi 15945. Mittauksen kohteena oli laboratorion paikallisverkon 10 Mbit/s ethernet-segmentti. Mitatusta liikenteestä puuttuu laboratorion LAN-emuloidun paikallisverkon sisäinen liikenne. Tämä emuloidun lähiverkon sisäinen liikenne voidaan kuitenkin katsoa niin vähäiseksi, ettei sillä juurikaan ole vaikutusta mittaustuloksiin. Tarkempi kuva mitatusta verkosta on esitetty liitteessä 2. Mittaustulosten analyysi perustui samoille periaatteille kuin edellä esitetty suuren runkoverkon analyysi. Aluksi tutkittiin ainoastaan IP-osoitepareja ja tehtiin tästä yksinkertainen vuoanalyysi, jonka eräs tulos on esitetty kuvassa 6-6.



Kuva 6-6: Kumulatiivinen voiden ja pakettien jakauma lähiverkossa vuon elinaikaan verrattuna

Kuvasta 6-6 nähdään, että likimain 50 % edellä mainituin perustein muodostetuista voista on alle minuutin mittaisia ja näissä siirtyy noin 30 % kaikista paketeista. Jos tarkastellaan sitä 10 % osuutta, joka muodostaa kaikkein pitkäkestoisimmat vuot, huomataan, että näillä voilla siirtyy noin 45 % kaikista paketeista.

Protokolla-analyysiä varten mukaan otetaan ne protokollat, joiden muodostamien yhteyksien siirretty pakettimäärä on 0,05 % kaikista lähetetyistä paketeista. Protokolla-analyysiin saadaan näin mukaan 99,88 % kaikista lähetetyistä paketeista. Analyysin tulokset on esitetty taulukossa 6-5.

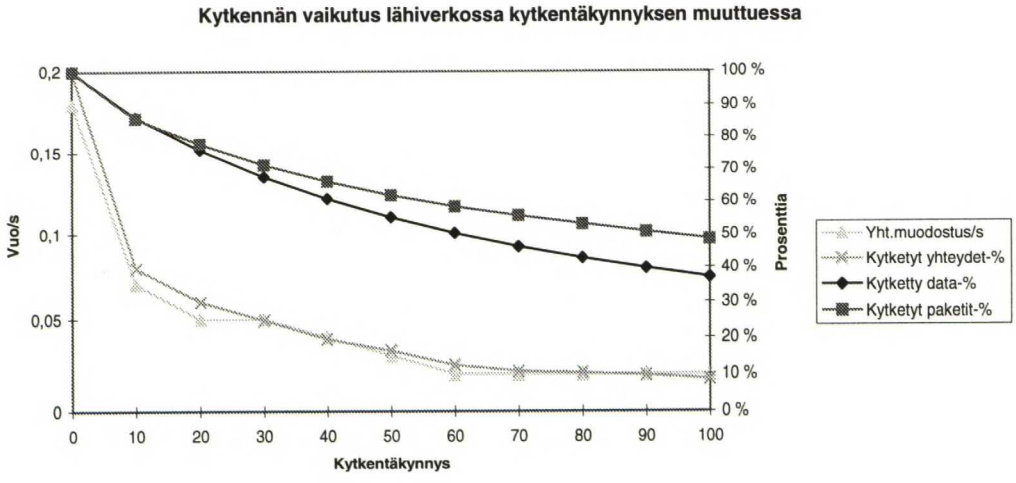
Taulukko 6-5: Lähiverkon liikenteen protokolla-analyysi

Protokolla	Portti	Kytkentä	%vuo	%paketti	%tavu	vuo/s	paketti/s	Keskim.kesto	Paketti/vuo
TCP/ssh	*22*	*	7,21 %	16,59 %	12,19 %	0,005	0,22	197,1	44
TCP/http	*80*		46,39 %	42,62 %	63,55 %	0,009	0,15	117,0	18
?	*5136*		1,56 %	0,24 %	0,04 %	0,005	0,01	211,2	3
TCP/telnet	*23*		0,96 %	0,77 %	0,09 %	0,004	0,06	249,5	15
UDP/dns	*53*		11,18 %	1,71 %	0,78 %	0,011	0,03	89,4	3
TCP/pop-3	*110*		1,20 %	0,63 %	0,04 %	2,179	22,00	0,5	10
TCP/www-proxy	*8000*		3,37 %	3,07 %	5,52 %	0,001	0,03	671,7	17
TCP/X-11	*60xx*	*	5,29 %	28,34 %	14,43 %	0,008	0,85	121,4	103
stun-port	*1994*		0,24 %	0,16 %	0,20 %	0,120	1,50	8,4	13
TCP/nntp	*119*		0,36 %	0,12 %	0,23 %	0,020	0,13	49,3	6
UDP/finger	*79*		0,96 %	0,25 %	0,14 %	21,739	108,70	0,0	5
TCP/smtp	*25*		1,20 %	0,96 %	0,36 %	0,015	0,23	65,7	15
nfs			0,96 %	0,18 %	0,29 %	0,007	0,03	136,6	4
UDP/sunrpc	*111*		0,72 %	0,08 %	0,03 %	0,003	0,01	360,1	2
TCP/netbios-dgm	*138*		8,29 %	1,39 %	1,45 %	0,005	0,02	188,2	3
TCP/netbios-ns	*137*		6,73 %	1,70 %	0,52 %	0,015	0,07	68,9	5
UDP/route		*	0,36 %	0,85 %	0,00 %	0,001	0,03	1343,6	45
UDP/timed	*525*		0,60 %	0,06 %	0,02 %	0,005	0,01	191,8	2
UDP/who	*513*		1,68 %	0,18 %	0,10 %	0,008	0,02	132,9	2

Yhteyden kytkemisehdot on esitetty taulukossa 6-3. Kun näitä ehtoja sovelletaan on havaittu, että noin 46 % kaikesta liikenteestä voidaan kytkeä omille virtuaaliyh-

teyksilleen. Nämä vuot muodostavat 13 % kaikista voista ja koska yhden vuon muodostamiseen tarvitaan noin 10 pakettia muodostuu tämä kuorma kohtuulliseksi. Vuonmuodostusnopeudeksi vaaditaan tässä tilanteessa 0,051 vuota sekunnissa. Mikäli vuo muodostettaisiin kaikille havaituille voille, olisi vuonmuodostusnopeus noin 0,4 vuota sekunnissa. Protokolla-analyysin tuoma kuormanpienennys vuonmuodostuksessa on siis noin 87 %. Jos kytkettäviin voihin otetaan mukaan kaksi seuraavaksi kytkentään soveltuvinta protokollaa (http, www-proxy) saadaan vuonmuodostusnopeudeksi noin 0,25 vuota sekunnissa ja kuormanpienennys vuonmuodostuksessa on noin 37 %.

Tarkasteltaessa vuon kytkemisehtoa siten, että tarkkaillaan vuolla lähetettyjen pakettien määrää ja kytketään vuo omalle virtuaaliyhteydelleen tietyn saapuneen pakettimäärän jälkeen, voidaan tarkastella tämän ns. kytkentäkynnyksen vaikutusta vuonmuodostukseen ja kytketyillä yhteyksillä välitettyjen pakettien ja tiedon määrään. Tämä tarkastelu on tehty kuvassa 6-7.

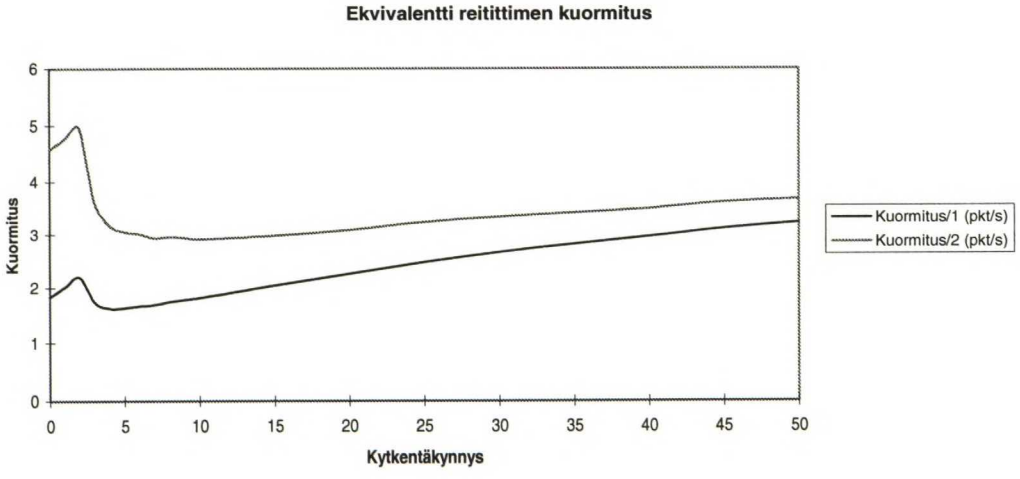


Kuva 6-7: Kytkentäkynnyksen vaikutus vuon muodostukseen runkoverkossa

Etsittäessä kytkentäkynnyksen arvoa, jolla päästäisiin samaan vuonmuodostusnopeuteen, kuin protokolla-analyysin perusteella saadaan kuvan 6-7 perusteella kytkentäkynnyksen arvoksi noin 20 pakettia. Erityisesti on huomattava, että mikäli vuoluokittelu perustuu puhtaasti protokolla-analyysiin, vuonmuodostuksessa aiheutuva teoreettinen maksimikuorma on noin 122 % suurempi, kuin jos vuonmuodostus tehdään pelkästään vastaanotettujen pakettien määrän perusteella. Tämä johtuu protokolla-analyysin sokeudesta tavallisesti pitkiä yhteyksiä sisältävissä

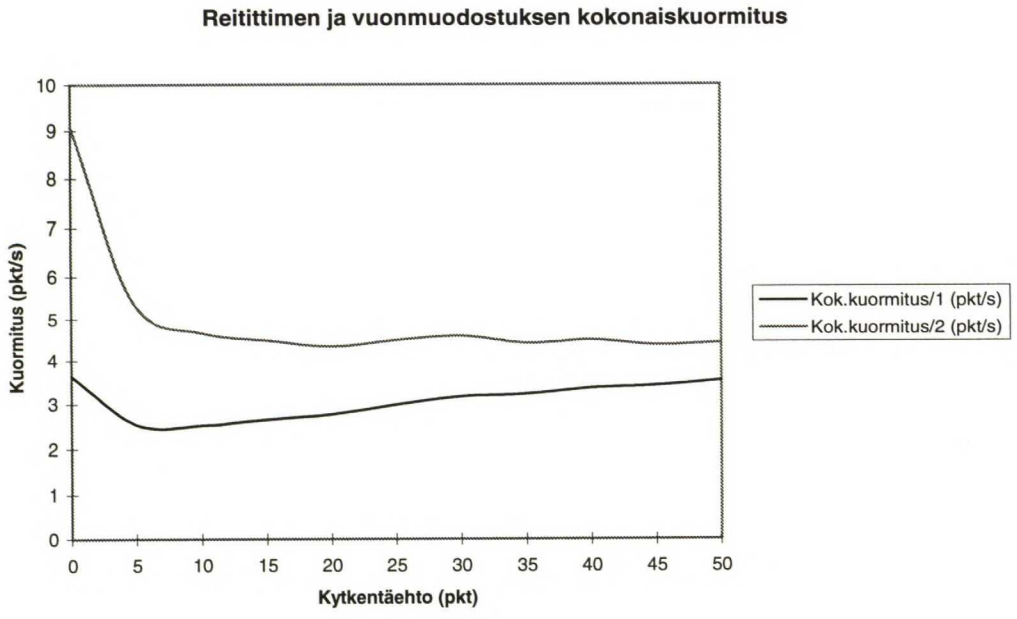
protokollissa esiintyville lyhytaikaisille, ja siten vain muutamia paketteja sisältäville, yhteyksille.

Reitityskomponentin kuormitus kytkentäkynnyksen funktiona 10 paketin ja 25 paketin vuonmuodostuksella on esitetty kuvassa 6-8.



Kuva 6-8: Reititysfunktion kuormitus 10 paketin (kuormitus/1) ja 25 paketin (kuormitus/2) kytkentäkynnyksillä

Kuvasta 6-8 havaitaan, että kuormitusfunktiolla on minimi 10 paketin ja 25 paketin yhteydenmuodostuksella vastaavasti 5 paketin ja 10 paketin kytkentäkynnyksen kohdalla. Verrattaessa reititysprosessorin tekemää työtä täysin reitittävässä ympäristössä ja IP-kytkentää hyödyntävässä ympäristössä saavutetaan vastaavasti 80 % ja yli 60 % vähennys reitityskomponentin tekemälle työlle. Viimeiseksi tarkastellaan reitityskomponenttia ja vuonmuodostuskomponenttia yhtenä kokonaisuutena, jonka kokonaiskuormitusta pyritään minimoimaan. Tällainen tarkastelu on esitetty kuvassa 6-9.



Kuva 6-9: Kokonaiskuormitus reitittimessä ja vuonmuodostajassa 10 paketin (kuormitus/1) ja 25 paketin (kuormitus 2) vuonmuodostuksella

Kuvasta havaitaan, että reititys- ja vuonmuodostuskomponenttien toiminta on optimaalista, kun on vastaanotettu 7 tai 20 pakettia riippuen siitä, vaatiiko vuonmuodostus 10 tai 25 pakettia.

6.3 Yhteenveto liikennemittauksista

Liikennemittauksissa käytettiin analysoinnin mallina suuresta runkoverkosta tehtyä mittausta. Tämän työn puitteissa mittaukset tehtiin kahdessa fyysiseltä siirtonopeudeltaan samanlaisessa, mutta käyttäjämäärältään hyvin erilaisessa verkossa. Verkoissa havaitut yhteydellisen tason protokollat olivat kahden pienemmän verkon kesken melko samanlaisia, mutta erosivat suuren runkoverkon välittämistä protokollista. Tämä johtuu mittausajankohtien huomattavasta välistä ja verkkojen käyttäjien erilaisuudesta. Protokollien suhteelliset osuudet lähetetyistä paketeista erosivat runkoverkon ja pienempien verkkojen osalta, mutta pienempien verkkojen keskinäinen vertailu antaa samaa suuruusluokkaa olevia protokollien suhteellisia osuuksia. Jälkimmäistä seikkaa voidaan selittää sillä, että lähiverkko on osa pienempää runkoverkkoa ja muodostaa myös osan pienen runkoverkon liikenteestä.

Sovellettaessa erilaisia luokitteluperusteita voitiin havaita, että liikenne on merkittävässä määrin yhteydellistä ja niinmuodoin sopivaa kytkentäisten tekniikoiden soveltamiseen. Tulosten lukuarvoista nähdään suoraan, että kaikki nykyiset internet protokollia ATM-verkoissa välittävät ratkaisut selviävät teknisesti lähiverkkojen ja pienten runkoverkkojen tuottamasta liikennekuormasta helposti. Tärkeämpää onkin selvittää, mitkä ratkaisut ja periaatteet soveltuvat parhaiten aina eri kokoluokkien tietoliikenneverkkoihin.

Lopuksi on huomattava, että tämän työn puitteissa on tehty vain kaksi mittausta, jotka on analysoitu tarkasti. Tämän katsotaan kuitenkin riittävän, silloin kun pyritään määrittämään tiettyjen liikenteen välitysmenetelmien sopivuutta eri kokoluokkien verkkoihin. Yleisten liikenneteoreettisten trendien ja ominaisuuksien etsinnässä täytyisi mittauksia tehdä huomattavasti enemmän.

Liikennemittausten analyysin perusteella saadut tulokset on esitetty kootusti taulukossa 6-6.

Taulukko 6-6: Mittaustulosten yhteenveto

	Runkoverkko	Runkoverkko (Sähköosasto)	Lähiverkko
Lyhyet yhteydet ja pakettien osuus näillä	64% < 1 min. 16% paketeista	50% < 20 s 30% paketeista	50% < 1 min. 30% paketeista
Pitkät yhteydet ja pakettien osuus näillä	10% pisimmistä 50% paketeista	10 % pisimmistä 50% paketeista	10% pisimmistä 45 % paketeista
Kytkettävien pkt. osuus	70, 77%	52,16%	45,78%
Muodostettujen voiden osuus havaituista	21,32 %	18,42%	12,86 %
Vuonmuodostusnopeus (protokolla-analyysi)	92 vuota/s	0,9 vuota/s	0,051 vuota/s
Kytkentäkynnys em. vuonmuodostusnopeudelle	13 pkt	≈20 pkt	20 pkt
Kytkentäkynnys kokonaiskuormitusminimissä (10 pkt/vuo)	ei määritettävissä tarkasti	12 pkt	7 pkt
Kytkentäkynnys kokonaiskuormitusminimissä (25 pkt/vuo)	ei määritettävissä tarkasti	22 pkt	20 pkt
Reitityskuorman pienentyminen (vuonmuodostuskuorma 10 pkt/vuo)	80 %	90 %	80 %
Vuonmuodostuskuorman pieneneminen (protokolla-analyysi)	ei määritettävissä tarkasti	78 %	87 %

Johtopäätökset

Liikennemittaukset

Liikennemittausten perusteella voidaan katsoa, että internet-verkkojen liikenne on luonteeltaan suurelta osin yhteydellistä. Kaikissa internet-liikennettä välittävissä eri kokoluokan verkoissa jopa puolet verkossa tapahtuvasta pakettien välityksestä voitaisiin hyvin ohjata omille yhteyksilleen. Yhteydelliset siirtotekniikat, ja mielellään sellaiset, jotka tarjoavat dynaamisesti tapahtuvan siirtokaistan jakamisen käyttäjien kesken, ovat internet-liikenteen tehokkaalle välitykselle välttämättömyys. ATM-tekniikka soveltuu eri kokoluokan tietokoneverkkojen ja näitä yhdistävien runkoyhteyksien siirtotekniikaksi erittäin hyvin, kun näissä verkoissa käytetään internet-protokollia.

ATM-tekniikkaa soveltavia ratkaisuja internet-liikenteen välitykseen on kuitenkin useita ja valinta näiden välillä voi muodostua pulmalliseksi. Liikennemittausten perusteella voidaan sanoa, että mitkään kaksi tietokoneverkkoa eivät ole keskenään samanlaiset. Verkon käyttäjien mieltymykset, työtavat ja käytetyt ohjelmistot muuttavat verkon palveluprofiilia oleellisesti tarkasteltaessa erilaisissa verkoissa esiintyvää liikennettä. Uudet vasta käyttöönotetut sovellukset, jotka kohottavat verkon tietoturvaa, peittävät alleen käytettyjen verkkopalveluiden monimuotoisuuden. Toisaalta aivan uudenlaisia sovelluksia syntyy nopeassa tahdissa, eikä voida varmasti sanoa, miltä internet-verkon liikenne palvelujen käytön näkökulmasta näyttää esimerkiksi viiden vuoden kuluttua.

Yhteyksien eli tietovoiden muodostaminen asettaa erilaisille tekniikoille haasteen tehdä yhteyksien havainnointi ja mahdollinen vuoluokittelu niin joustavaksi, että se soveltuisi käytettäväksi erilaisissa verkkoympäristöissä. Toisaalta mikäli vuoluokittelun menetelmät muuttuvat liian monimutkaisiksi ja moninaisiksi menetetään helposti voiden muodostamisen mukanaan tuomat edut.

Uudet tekniikat antavat mahdollisuuden jakaa liikenteen välityksestä aiheutuvaa kuormaa tasaisemmin verkon eri komponenteille, mutta toisaalta laitteistoja ohjaavat ohjelmistot nousevat merkittävään asemaan liikenteen välityksen onnistumisen kannalta.

IP over ATM

IP over ATM -ratkaisu sopii hyvin eri kokoluokan verkkoihin, mutta toisaalta verkkoon ei voida liittää *IP over ATM* -ratkaisua tukemattomia laitteita, vaikka ne pystyisivätkin käyttämään hyödyksi ATM-tekniikkaa. Monilähetyksen puutteellinen standardointi ja tekniikan kykenemättömyys taata erilaisia palvelun tasoja estää tämän ratkaisun laajemman leviämisen. Lisäksi ratkaisu tuhlaa verkon kapasiteettia varaamalla sitä hyvin pitkiksi ajoiksi suhteessa keskimääräisiin yhteyden pituuksiin. Suomessa *IP over ATM* -ratkaisu on käytössä Suomen korkeakouluja ja yliopistoja yhdistävän FUNET-verkon runkoverkkoratkaisuna. *IP over ATM* -ratkaisu soveltuukin hyvin sellaisiin verkkoihin, joissa liikennettä on paljon, mutta lukumääräisesti harvoihin kohteisiin. Tutkimusverkoissa ja eri kokoluokan hallituissa ympäristöissä *IP over ATM* -ratkaisu puolustaa paikkaansa, mutta minimaalisen reitityskapasiteetin omaavana teknologiana se ei sovellu verkon keskeisiin solmukohtiin. Toisaalta suurta liikennemäärää yksittäisiin verkon solmukohtiin kuljettavat verkon osat voidaan hyvin toteuttaa *IP over ATM* -ratkaisun avulla. *IP over ATM* -ratkaisu tulee näin ollen jäämään yksinkertaisten tutkimusverkkojen sekä suurten ja selkeiden runkoverkkojen tekniikaksi.

ATM Forumin lähiverkkoemulaatio

Lähiverkkoemulaatio on raskas toteuttaa; protokollien ja verkkoelementtien runsaus kuormittaa laitteita ja kuluttaa siirtokapasiteettia verkosta. Lähiverkkoemulaatio ei tue palvelun laatua verkossa, joten se ei sovellu palvelun laatua vaativille sovelluksille verkoissa, joissa kapasiteetin käyttö on jo maksimaalista. Ratkaisu lieneekin suunniteltu pieniä, mutta tehokkaita, komponentteja sisältäviä työasemaverkkoja varten ja toisaalta helpottamaan ATM-tekniikan läpimurtoa.

Yhteydettömän palvelun emuloiminen yhteydellisellä tekniikalla on jo sinänsä paradoksaalista, ja onkin erittäin todennäköistä, että lähiverkkoemulaatio tulee väistymään erilaisten kytkentäisten tekniikoiden tieltä myös lähiverkkoympäristöissä. Runkoverkoihin lähiverkkoemulaatio ei sovellu reititysominaisuuksien puutteen vuoksi. ATM Forumin lähiverkkoemulaation tulevat versiot lupaavat tehokkaita reititysominaisuuksia, mutta jää nähtäväksi kykenevätkö nämä tehokkaampaan reititykseen internet-reititysprotokollien rinnalla.

IP-kytkentä

Idea IP-osoiteparien välille muodostettavista yhteyksistä on yksinkertaisuudessaan hyvä, mutta tehtyjen mittausten perusteella soveltuvuus erikokoisiin verkkoihin vaatii tekniikalta ennenkaikkea joustavuutta. Eri kokoluokan verkkojen palveluprofiilit ovat hyvin erilaisia ja asettavat suuria vaatimuksia vuoluokittelun määrittelylle ja muutosmahdollisuuksille itse IP-kytkentälaitteistoissa. Tietovuon kytkemispäätöksen tulee IP-kytkentää tukevissa laitteissa kuitenkin pohjautua samoihin perusteisiin yhdessä verkkoympäristössä, mikäli mielitään saada kunnollista parannusta verkon välityskykyyn. Mikäli vuoluokittelun perusteet ovat esimerkiksi verkon vierekkäisissä elementeissä erilaisia, ei IP-kytkentää välttämättä pystytä edes muodostamaan.

IP-kytkennän sovellusalueet poikkeavat selvästi edellä esitetystä lähiverkkoemulaatiosta ja ovat osittain samoilla linjoilla *IP over ATM* -ratkaisun kanssa. IP-kytkentä, sellaisena kuin se tässä työssä on esitetty, tarjoaa menetelmän pienentää reitittimien aiheuttamaa viivettä tietokoneverkoissa. Ipsilon-ympäristöstä on kuitenkin mahdoton saada suorituskykyparannuksia, ellei verkko kokonaisuudessaan, tai ainakin hyvin suurilta osin, tue Ipsilon-protokollia. Jotta Ipsilon-ympäristöstä saavutettaisiin täysi hyöty, tarvitaan vähintään kolme laitetta, jotka tukevat IFMP-protokollaa; tutkimusympäristöjä voidaan toki perustaa kahdenkin laitteen varaan, mikäli näiden välille voidaan muodostaa silmukoita. Tämän takia tulevaisuuden IP-kytkentäratkaisujen suunnittelun yhteydessä tuleekin huolellisesti paneutua yhteensopivuuden takaamiseen muiden ATM-tekniikkaa hyödyntävien ratkaisujen kanssa.

Tällä hetkellä IP-kytkentä soveltuu parhaiten isojen ja pienten runkoverkkojen toiminnan yleiseen tehostamiseen ja toisaalta reitittimien suorituskyvyn osalta kriittisiin runkoverkkojen solmukohtiin. Reitittimille, jotka muodostavat nykypäivän verkoissa usein pahimmat pullonkaulat, IP-kytkentä lupaa vähintäänkin noin 60 % helpotusta työkuormaan. Useissa tapauksissa reitittimien kuorman pienentyminen on vieläkin näkyvämpää. Täyden hyödyn saavuttamiseksi täytyy kriittinen kohta kuitenkin ympäröidä Ipsilon-laitteistoilla, mikä ei aina ole mahdollista.

Suorituskyvyn parantumisen edellytyksenä IP-kytkentää käyttävissä verkoissa on myös se, että palveluprofiili on yhteydellinen, so. liikenne muodostuu sellaisista liikennevirroista, jotka ovat pitkäikäisiä ja joilla tapahtuu kohtuullisen paljon tie-

donsiirtoa. Tällöin uusien voiden luontia ja purkamista tapahtuu huomattavasti harvemmin, kuin sellaisessa ympäristössä, jossa jokaiselle IP-osoiteparille muodostetaan oma yhteys. Samassa yhteydessä tulee kiinnittää huomiota vuoluokittelun erilaisten menetelmien tehostamiseen ja uusien joustavien menetelmien kehittämiseen.

Mikäli vuoluokittelu perustuu yksinomaan protokolla-analyysien pohjalta saatuihin tuloksiin, on vaarana se, että sellaisetkin yhteydet kytketään, joiden elinaika on tosiasiallisesti lyhyt. Niin ikään liikenteen palveluprofiilin muutoksiin reagoiminen vaikeutuu. Toisaalta, jos kytkemispäätökset perustuvat yksinomaan reititinkomponenttien kokonaiskuormituksen minimoimiseen, voi kuormitus kasautua puolestaan vuonmuodostuskomponentille. Käyttäjälle tilanne näkyy verkon palvelutason laskuna, oli kuormitettu komponentti mikä hyvänsä.

Tämän työn tulosten perusteella on suositeltavaa tehdä vuonmuodostuspäätökset pienissä verkoissa yksinomaan yhteydellä lähetettyjen pakettien määrän perusteella eli reititinkomponentin työn minimoimiseksi. Vuonmuodostuksen absoluuttiset arvot eivät tässä mitatuissa verkoissa kasva liian suuriksi, vaikka näin meneteltäisiinkin. Verkon koon ja yhteyksien määrän kasvaessa täytyy vuonmuodostuksessa ottaa myös huomioon välitettävän liikenteen protokollaprofiili. Parhaaseen tulokseen, jossa optimoidaan sekä reitityksen että vuonmuodostuksen kuormitus, päästään yhdistämällä protokolla-analyysi ja kokonaiskuormituksen minimointi. Tällöin protokolla-analyysi tarjoaa menetelmän tyypillisesti pitkien IP-voiden tunnistamiseen ja kytkentäkynnys takaa sen, ettei kyseessä ole yhteys, jolla lähetettäisiin lukumääräisesti vähän paketteja tyypillisesti paljon paketteja sisältävillä protokollilla.

Erityisesti on huomattava, että pienen kokoluokan verkoissa, liikenteen monimuotoisuudesta ja toisaalta vuoluokittelun joustamattomuudesta johtuen, IP-kytkentä ei välttämättä kykene käyttämään kaikkea potentiaaliaan. Liikenteen protokollaprofiilin vaihtelut ovat pienissä verkoissa niin suuria, että pelkkään protokolla-analyysiin pohjautuva vuoluokittelu ei pysy alati muuttuvan internet-liikenteen tahdissa.

Loppupäätelmät

Palvelun laatu muodostuu tulevaisuuden sovelluksille ja niiden käyttäjille tärkeäksi, joten internet-liikennettä välittävien järjestelmien tulee pystyä takaamaan tarvittaessa vaadittu palvelun taso. Tällä hetkellä internet-liikennettä siirretään kuitenkin suurelta osin siirtomediaa jakavilla tekniikoilla (CSMA/CD, Token Ring) ja lisäksi verkon solmukohtien reitittimet eivät hyödynnä internet-liikenteen selkeää yhteydellistä luonnetta. ATM-tekniikan avulla voidaan muodostaa yhteyksiä, joita muut käyttäjät eivät, ainakaan periaatteessa, pysty häiritsemään. Yhteyskerroksen palvelutason erottimia (TCP-portit, ToS-bitit) voitaisiin jo nyt käyttää palveluluokkien riittävän tarkkaan jaotteluun. Uusien verkkokerroksen protokollien (IPv6) tullessa käyttöön voidaan palvelun laatu verkkotasonkin protokollien puolesta toteuttaa. Toisaalta nykyisenkaltainen IP-kytkentä ei takaa, että palvelun laatu olisi sama kaikissa verkkoelementeissä; kytkettäessä IP-vuota omalle yhteydelleen ei tiedetä, mitkä ovat palveluparametrit muilla yhteyden osilla. Tätä epäkohtaa pystyttäisiin parantamaan, mikäli tutkittaisiin mahdollisuuksia käyttää merkinantoa IP-kytkennän kanssa.

Vaikka IP-kytkentä mukautuu kohtuullisen hyvin erikokoisiin verkkoihin, uusien palvelujen ja toisaalta tietoturvalle asetettujen vaatimusten mukana verkossa käytettävät protokollat ja niiden keskinäiset suhteet voivat muuttua nopeassakin tahdissa. Tästä ovat hyvänä esimerkkinä erilaiset reaaliaikaiset ääni- ja kuvapalvelut internet-verkoissa. Tämäntyyppiset palvelut soveltuvat erittäin hyvin kytkentäisiin ympäristöihin. Tällä hetkellä IP-kytkentäratkaisut, ja erityisesti vuoluokittelu, nojaavat liian vahvasti jo tehtyihin mittauksiin ja mittaustuloksiin sekä niistä tehtyihin päätelmiin. IP-kytkentää siinä muodossa, kuin se tässä työssä on esitetty, tulee kehittää voimakkaasti joustavampaan suuntaan erityisesti voiden havainnoinnin, luokittelun ja kytkemisperusteiden osalta. Tämä mahdollistaisi yksittäisten tietoliikenneverkkojen ominaispiirteiden huomioinnin ja mahdollistaisi IP-kytkennän tehokkaan hyödyntämisen kaikissa verkkoympäristöissä.

Lähdeluettelo

/1/ Chen, Thomas M & Liu, Stephen S. ATM Switching Systems. USA. Artech House Inc. 1995. 261 s. ISBN 0-89006-682-5.

/2/ Stallings, William. ISDN and Broadband ISDN. 2nd ed. Macmillan Publishing Company. 1992. 633 s. ISBN 0-02-415475-X.

/3/ Halsall, Fred. Data Communications, Computer Networks and Open Systems. 4th ed. USA. Addison-Wesley Publishing Company Inc. 1996. 899 s. ISBN 0-201-42293-X.

/4/ Stallings, William. Data and Computer Communications. 4th ed. Macmillan Publishing Company. 1994. 875 s. ISBN 0-02-415441-5.

/5/ AF95-0013R10. Traffic Management Spesification Version 4.0. ATM FORUM. 1995.

/6/ RFC 791: Internet Protocol DARPA Internet Program Protocol Specification. Information Sciences Institute. University of Southern California, 1981.

/7/ RFC 1812: Requirements for IP version 4 Routers. 1995.

/8/ Comer, Douglas E. Internetworking With TCP/IP. Prentice-Hall, Inc. 1988.

/9/ RFC 1883: Internet Protocol, Version 6 (IPv6) Specification. 1995.

/10/ RFC 793: Transmission Control Protocol DARPA Internet Program Protocol Specification. Information Sciences Institute, University of Southern California. 1981.

/11/ RFC 768: User Datagram Protocol. 1980.

/12/ RFC 1932: IP over ATM: A Framework Document. 1996.

/13/ Saarelainen, Kari. Lähiverkkojen tekniikka.Yritysmikrot Oy. 1993. 358 s. ISBN 952-9508-12-3.

/14/ RFC 1483: Multiprotocol Encapsulation over ATM Adaptation Layer 5. 1993.

/15/ RFC 1577: Classical IP and ARP over ATM. 1994.

/16/ RFC 1755: ATM Signalling Support for IP over ATM. 1995.

/17/ Alles, A. ATM Internetworking. Cisco Systems, Inc. 1995.

/18/ AF-LANE-0021.00. LAN Emulation Over ATM Version 1.0. ATM FORUM. 1995.

/19/ IP Switching: The Intelligence of Routing, the Performance of Switching. Technical White Paper on IP switching. Ipsilon Networks, Inc. USA. 1996.

/20/ Minshall, Lyon, Newman Peter. Flow Labelled IP: Connectionless ATM under IP. Ipsilon Networks, Inc. USA. 1996.

/21/ Claffy, Braun, Polyzos. A parameterizable methodology for Internet traffic flow profiling. IEEE Journal of Selected Areas in Communication 13(8). Oct. 1995, pp.1481-1494.

/22/ RFC 1954: Transmission of Flow Labelled IPv4 on ATM Data Links. 1996.

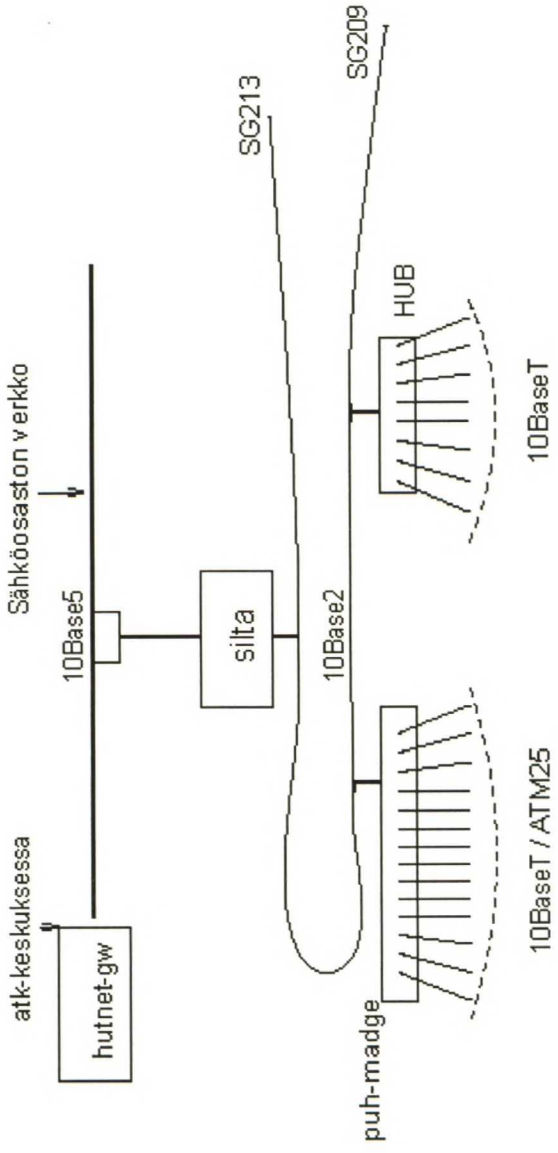
/23/ RFC 1953: Ipsilon Flow Management Protocol Spesification for IPv4. 1996.

/24/ RFC 1987: Ipsilon's General Switch Management Protocol Spesification. 1996.

Liite 1: TCPDUMP-ohjelman tulostiedoston osa

```
09:58:15.323529 puh-pc36.hut.fi.1185 > www.ipsilon.com.80: . ack 1
win 8576 (DF)
09:58:15.333529  puh-pc36.hut.fi.1185  >  www.ipsilon.com.80:  P
1:174(173) ack 1 win 8576 (DF)
09:58:15.663529 www.ipsilon.com.80 > puh-pc36.hut.fi.1185: . ack
174 win 3923
09:58:15.813529  www.ipsilon.com.80  >  puh-pc36.hut.fi.1185:  .
1:513(512) ack 174 win 4096
09:58:15.813529  www.ipsilon.com.80  >  puh-pc36.hut.fi.1185:  .
513:1025(512) ack 174 win 4096
09:58:15.813529 puh-pc36.hut.fi.1185 > www.ipsilon.com.80: . ack
1025 win 8576 (DF)
09:58:16.003529  www.ipsilon.com.80  >  puh-pc36.hut.fi.1185:  .
1025:1537(512) ack 174 win 4096
09:58:16.003529  www.ipsilon.com.80  >  puh-pc36.hut.fi.1185:  .
1537:2049(512) ack 174 win 4096
09:58:16.003529  www.ipsilon.com.80  >  puh-pc36.hut.fi.1185:  FP
2049:2188(139) ack 174 win 4096
09:58:16.003529 puh-pc36.hut.fi.1185 > www.ipsilon.com.80: . ack
2189 win 8576 (DF)
09:58:16.083529  puh-pc36.hut.fi.1186  >  www.ipsilon.com.80:  S
8274508:8274508(0) win 8192 <mss 1460> (DF)
09:58:16.093529  puh-pc36.hut.fi.1187  >  www.ipsilon.com.80:  S
8274518:8274518(0) win 8192 <mss 1460> (DF)
09:58:16.103529  puh-pc36.hut.fi.1188  >  www.ipsilon.com.80:  S
8274527:8274527(0) win 8192 <mss 1460> (DF)
09:58:16.123529  puh-pc36.hut.fi.1185  >  www.ipsilon.com.80:  R
8273728:8273728(0) win 0 (DF)
09:58:16.133529  puh-pc36.hut.fi.1189  >  www.ipsilon.com.80:  S
8274552:8274552(0) win 8192 <mss 1460> (DF)
09:58:16.273529  www.ipsilon.com.80  >  puh-pc36.hut.fi.1186:  S
1453824000:1453824000(0) ack 8274509 win 4096
09:58:16.273529 puh-pc36.hut.fi.1186 > www.ipsilon.com.80: . ack 1
win 8576 (DF)
09:58:16.273529  www.ipsilon.com.80  >  puh-pc36.hut.fi.1187:  S
1453888000:1453888000(0) ack 8274519 win 4096
09:58:16.273529 puh-pc36.hut.fi.1187 > www.ipsilon.com.80: . ack 1
win 8576 (DF)
09:58:16.283529  puh-pc36.hut.fi.1186  >  www.ipsilon.com.80:  P
1:222(221) ack 1 win 8576 (DF)
```

Liite 2: Teletekniikan laboratorion lähiverkko



Lähde: Peuhkuri, Markus. Teletekniikan erikoistyö II. Teknillinen Korkeakoulu, Teletekniikan laboratorio. 1996.